

DEMO

IT-Security
Sicherheit im Umgang
mit Informations- und
Kommunikationstechnologien

ISBN 978-3-85168-071-3

1. Auflage
Version: 1.0
2011

Verlag

bit media e-Learning solution GmbH & Co KG

Kärntner Straße 311
A-8054 Graz – Austria

e-Mail: office@bitmedia.cc

bit
best in training

Unsere Web-Adresse:
<http://www.bitmedia.com>

Das Werk und seine Teile sind urheberrechtlich geschützt. Jede Verwertung in anderen als den gesetzlich zugelassenen Fällen bedarf deshalb der vorherigen schriftlichen Einwilligung des Verlages.

Aufgrund der leichteren Lesbarkeit wird in dieser Unterlage auf eine Formulierung, die beide Geschlechter berücksichtigt, verzichtet und die Bezeichnung „Lernender, Benutzer, etc.“ verwendet. Dies soll keineswegs als Diskriminierung der einen oder anderen Form verstanden werden.

Autor: Michael Paulus

Fotoquelle: www.photocase.de

1. Auflage/Version 1.0

© 2011 by bit media e-Learning solution

Vorwort

Gute IT-Kenntnisse sind heute bereits eine Grundvoraussetzung um am Arbeitsmarkt bestehen zu können. Auch im Schul- und Ausbildungsbereich ist das Arbeiten mit dem PC zu einem fixen Bestandteil geworden.

Diese Lernunterlage fokussiert zweierlei:

Die Unterlage möchte Sie einerseits sattelfest für die IT-Welt machen, Ihnen andererseits den Zugang zu den Vorteilen eines gewandten Umgangs mit dem Computer eröffnen - PC Know-How und sichere Programmbedienung als Motor für effizientes und Freude bringendes Arbeiten.

Um die Brücke zwischen Theorie und Praxis zu schlagen, wurden die Inhalte der Unterlage bewusst handlungsorientiert gestaltet – so wird es Ihnen möglich sein, Ihr erlangtes Wissen, direkt in der täglichen Praxis anzuwenden.

Möchten Sie Ihre IT-Kenntnisse auf multimedialem Weg vertiefen, über Programmsimulationen und interaktive Übungen Ihr Wissen trainieren? Unsere e-Learning Produktpalette bietet Lernprogramme zu unzähligen IT-, aber auch Sprach- und Wirtschaftsthemen.

Für nähere Informationen senden Sie bitte ein E-Mail an office@bitmedia.cc oder besuchen Sie uns im Internet unter <http://www.bitonline.com>.

Dieses Lehrwerk wurde mit hohem Augenmerk auf fachliche und didaktische Qualität entwickelt. Dennoch lassen sich Fehler nicht gänzlich ausschließen. Herausgeber, Verlag und Autoren können für fehlerhafte Inhalte und deren Konsequenzen weder irgendeine Haftung noch juristische Verantwortung übernehmen.

Das Verlagsteam ist jedoch um eine kontinuierliche Weiterentwicklung und Optimierung der Lernunterlage bemüht. In den Optimierungsprozess möchten wir auch Ihre Anregungen und Wünsche mit einfließen lassen. Das Team freut sich über Ihr Feedback: support@bitmedia.cc (Im Mailbetreff bitte die ISBN-Nummer angeben.).

Die Medien des Verlagshauses **bit media** e-Learning solution GmbH & Co KG können Verweise und Links zu Internetseiten anderer Anbieter beinhalten. Aufbau, Gestaltung und Inhalt dieser verlagsfremden Angebote entziehen sich dem Einflussbereich von **bit media** e-Learning solution GmbH & Co KG. Die Verantwortung hierfür obliegt gänzlich dem jeweiligen Anbieter.

Erklärung zum Buch

Empfohlene Vorkenntnisse

Vorkenntnisse aus Betriebssystemgrundlagen sind erforderlich.

Aufbau und Gestaltung der Lernunterlage

Um Ihnen die Orientierung und Handhabung der Lernunterlage zu erleichtern, folgen alle Kapitel einem einheitlichen Aufbau:

- ➔ **Kapiteleinleitung**
Überblick über das Kapitelthema, die angestrebten Handlungskompetenzen und Lernziele
- ➔ **In Unterthemen / Unterkapitel gegliederte Stoffpräsentation**
- ➔ **„Das Wichtigste in Kürze“**
Zusammenfassung der wichtigsten Kapitelinhalte
- ➔ **Lernkontrolle**
Fragebogen zur Wiederholung und Festigung von Kapitelinhalten

Im Anhang befinden sich:

- ➔ **Glossar**
Sammlung wichtiger Fachbegriffe (inklusive Begriffsbeschreibung). Alle für die Prüfung relevanten Begriffe werden hier nochmals erklärt.
- ➔ **Lösungsteil**
Lösungen zu den Lernkontrollfragen
- ➔ **Stichwortverzeichnis**
Aus dem Text gefilterte Schlüsselbegriffe – zusätzliche Orientierungshilfe.

Typografische Gestaltungsmittel:

- ➔ **Befehle, Schaltfläche, Menüs, Register etc.**
sind mit Hilfe von einfachen Hochkommas hervorgehoben und fett formatiert.
z.B. Menü '**Datei**', Befehl '**Speichern unter...**'
- ➔ **Programmspezifische Bezeichnungen und Benennungen**
sind mit typografischen Anführungszeichen gekennzeichnet. Z.B. Sprachauswahl - Sprache „Deutsch Deutschland“; Druckdialogfenster - Bereich „Druckauswahl:“

Symbole & Icons:

Über Symbole werden spezielle Inhalte für Sie optisch hervorgehoben:



Das !-Symbol hebt wichtige Schlussfolgerungen, Fachbegriffe, Basisinformationen etc. hervor.



Nützliche Tipps sind mit dem Tipp-Symbol markiert.



Fragen zum Verständnis und zur Lernzielkontrolle sind mit dem ?-Symbol versehen.



Das Häkchen-Symbol kennzeichnet die Zusammenfassung am Ende eines Kapitels.



Durch das Maus-Symbol sind Lerninhalte gekennzeichnet, zu denen es eine passende e-Learning Sequenz von bit media gibt.

Inhaltsverzeichnis

1	Datensicherheit – Grundlagen	9
1.1.	Daten und Informationen	9
1.1.1.	Eine etwas andere Definition von Daten und Informationen	9
1.1.2.	Informationsgesellschaft.....	11
1.2.	Datenzerstörung und Datenmissbrauch.....	12
1.3.	Cybercrime (Internetkriminalität)	13
1.3.1.	Von Personen ausgehende Gefahren	14
1.3.2.	Straftatbestände von Internetkriminalität	14
1.3.3.	Missbrauchsformen der Internetkriminalität.....	14
1.3.4.	Hacking	15
1.4.	Schutz von personenbezogenen Daten	16
1.4.1.	Datenschutz.....	16
1.4.2.	Bedeutung des Internets im Zusammenhang mit Datenschutz.....	17
1.4.3.	Datenschutzrichtlinie	17
1.4.4.	Maßnahmen und Richtlinien zum Datenschutz	18
1.4.5.	Datensicherheitsmerkmale	21
1.4.6.	Sicherheitsstrategien und Richtlinien	21
1.5.	Social Engineering	22
1.5.1.	Formen des Social Engineering.....	22
1.5.2.	Schutz vor manipulativen Telefonanrufen, Phishing oder Shoulder Surfing	24
1.6.	Identitätsmissbrauch	25
1.6.1.	Methoden des Identitätsmissbrauchs	25
1.7.	Sichere Dateien – ein Leitfaden	26
1.7.1.	Makro-Sicherheitseinstellungen.....	26
1.7.2.	Passwortschutz für Dateien	27
1.7.3.	Verschlüsselung.....	28
1.8.	Lernkontrolle.....	30
1.9.	Das Wichtigste in Kürze	31
2	Malware	33
2.1.	Was ist Malware?.....	33
2.2.	Malware - Typen	34
2.2.1.	Computerviren	34
2.2.2.	Arten der Infektion.....	35
2.2.3.	Computerwürmer.....	36
2.2.4.	Trojanisches Pferd (Trojaner).....	36
2.2.5.	Spyware.....	37
2.2.6.	Rootkit.....	38
2.2.7.	Backdoor	39

2.2.8.	Adware	39
2.2.9.	Botnet	39
2.2.10.	Keylogger	41
2.2.11.	Dialer	42
2.3.	Schutz vor Malware	42
2.3.1.	Funktionsweise von Antiviren-Software	44
2.3.2.	Grenzen der Antiviren-Software	46
2.4.	Lernkontrolle	47
2.5.	Das Wichtigste in Kürze	48
3	Sichere Netzwerke	49
3.1.	Netzwerk - Grundlagen	49
3.1.1.	OSI-Modell	50
3.1.2.	Kopplungs-Hardware	51
3.1.3.	Protokolle	54
3.1.4.	DNS (Domain Name System)	56
3.1.5.	Funktionsweise von Verschlüsselungen	58
3.2.	Netzwerk-Typen	63
3.2.1.	LAN (Local Area Network)	63
3.2.2.	MAN (Metropolitan Area Network)	64
3.2.3.	WAN (Wide Area Network)	64
3.2.4.	GAN (Global Area Network)	64
3.2.5.	VPN (Virtual Private Network)	65
3.2.6.	Mobiles VPN	66
3.2.7.	Leitungsgebundene Netze	66
3.2.8.	Funknetze	67
3.3.	Sicherheitsrichtlinien für drahtlose Netzwerke	69
3.3.1.	WEP (Wired Equivalent Privacy)	69
3.3.2.	Verbindung zu einem drahtlosen Netzwerk herstellen	69
3.4.	Netzwerk-Administration	71
3.4.1.	Der Netzwerkadministrator	71
3.4.2.	Authentifizierung	72
3.4.3.	Verwaltung von Benutzerrechten	72
3.4.4.	Dokumentation	72
3.5.	Firewall	73
3.5.1.	Externe Firewall	73
3.5.2.	Personal Firewall	74
3.6.	Kontrollierter Zugang zu Netzwerken	75
3.6.1.	Passwörter	76
3.6.2.	Pin-Code	76
3.6.3.	Allgemeine Richtlinien für gute Passwörter	76
3.6.4.	Weitere Richtlinien für gute Passwörter	77
3.6.5.	Biometrische Verfahren zur Zugangskontrolle	78
3.7.	Lernkontrolle	79
3.8.	Das Wichtigste in Kürze	80
4	Das WWW sicher nutzen	81
4.1.	Reale und „virtuelle“ Gefahren	81

4.1.1.	Risiken einschätzen	82
4.2.	Internetdienste.....	82
4.2.1.	WWW	82
4.2.2.	E-Mail.....	83
4.2.3.	FTP - Server.....	83
4.2.4.	Diskussionsforen	84
4.2.5.	Chat	84
4.2.6.	Telefonie per VoIP.....	84
4.2.7.	Fernsehen und Radio	84
4.2.8.	weitere Dienste.....	84
4.3.	Finanzielle Transaktionen per Internet	85
4.3.1.	Einmal-Kennwort	86
4.3.2.	Kennwortlisten.....	86
4.3.3.	Kennwortgeneratoren	86
4.4.	Pharming.....	87
4.4.1.	Die beim Pharming angewendete Methode	88
4.5.	Richtlinien sicherer Browser - Nutzung	88
4.5.1.	Digitales Zertifikat	88
4.5.2.	Überprüfung der Gültigkeit von Zertifikaten:	88
4.5.3.	Cookie.....	89
4.5.4.	InPrivate-Browsen.....	91
4.5.5.	Browserverlauf löschen.....	92
4.5.6.	Formulareingaben	93
4.5.7.	Inhaltskontrolle von Webangeboten	94
4.6.	Gefahrenpotentiale sozialer Netzwerke.....	96
4.6.1.	Vortäuschung falscher Tatsachen	96
4.6.2.	Cyber-Grooming	97
4.6.3.	Cyber-Mobbing.....	97
4.7.	Lernkontrolle.....	97
4.8.	Das Wichtigste in Kürze	98
5	Gefahren bei der Kommunikation.....	99
5.1.	Sicherer E-Mail-Verkehr	99
5.1.1.	E-Mail-Verschlüsselung	100
5.1.2.	Passwort-basierte E-Mail-Verschlüsselung	100
5.1.3.	PKI - Verfahren.....	100
5.1.4.	Die Signatur der E-Mail-Nachricht	102
5.1.5.	Verschlüsselung.....	102
5.1.6.	Entschlüsselung.....	103
5.1.7.	Überprüfung.....	104
5.2.	Digital signierte E-Mail unter MS Outlook	104
5.2.1.	Digital signieren auf Nachrichtenbasis	104
5.2.2.	E-Mail-Sicherheitseinstellungen	105
5.2.3.	Grundsätzliche Vorsichtsmaßnahmen bei eingegangenen E-Mails	106
5.2.4.	Phishing.....	107
5.2.5.	Vorsicht beim Öffnen von Attachments.....	107
5.3.	Risikominimierung bei Instant-Messaging	108
5.3.1.	Internet-Telefonie	108

5.3.2.	Instant-Messaging.....	108
5.3.3.	Einsatzgebiete von Instant-Messaging.....	109
5.3.4.	Gefahren und Sicherheits-Schwachstellen von Instant-Messaging.....	109
5.3.5.	Methoden, die Vertraulichkeit bei der Datenübertragung und die Authentizität des Gesprächs- bzw. Chat-Teilnehmers garantieren	109
5.4.	Lernkontrolle.....	111
5.5.	Das Wichtigste in Kürze	112
6	Datensicherung	113
6.1.	Hardware und Software inventarisieren	113
6.1.1.	Inventarlisten	114
6.2.	Grundlagen der Zugriffskontrolle.....	115
6.2.1.	Zugriffskontrolle	116
6.3.	Hardware und Software physisch schützen	117
6.3.1.	Zutrittskontrolle.....	117
6.3.2.	Sicherungskabel	118
6.4.	Daten digital schützen.....	119
6.4.1.	Authentifizierung.....	119
6.4.2.	Zugangskontrolle	119
6.5.	Daten-Backup	119
6.5.1.	Grundlegendes.....	120
6.5.2.	Überlegungen zu Speichermedien.....	121
6.5.3.	Gründe für Daten-Backup	121
6.5.4.	Gesetzliche Bestimmungen	121
6.5.5.	Konzept zur Datensicherung.....	122
6.5.6.	Arten des Backups.....	124
6.5.7.	Daten wiederherstellen und prüfen.....	124
6.6.	Lernkontrolle.....	125
6.7.	Das Wichtigste in Kürze	126
7	Absichtliche Datenvernichtung.....	127
7.1.	Sinn und Zweck der Datenvernichtung	127
7.2.	Daten löschen oder vernichten?.....	128
7.3.	Methoden der gezielten Datenvernichtung	130
7.3.1.	Software zur Datenvernichtung	130
7.3.2.	Entmagnetisierung.....	131
7.3.3.	Physische Zerstörung	131
7.4.	Lernkontrolle.....	132
7.5.	Das Wichtigste in Kürze	132
	Glossar.....	133
	Lösungen	137
	Index	140

Datensicherheit – Grundlagen

Die in Speichermedien eines Computers abgelegten Daten beinhalten Informationen, die vor Zerstörung, unberechtigtem Zugriff und missbräuchlicher Verwendung geschützt werden müssen.

Dieses Kapitel bietet einen Überblick über die wichtigsten Risiken bezüglich Datenverlust und Datendiebstahl und erklärt, wie Sie Ihre Daten und in weiterer Folge sich selber vor kriminellen Zugriffen schützen können.

- ➔ Szenarien der Datenzerstörung und des Datenmissbrauchs
- ➔ Informationen sind wertvoll und schützenswert
- ➔ Bedrohungen der persönlichen Sicherheit vermeiden
- ➔ Begriffe und Methoden des Social Engineerings und des Identitätsdiebstahls
- ➔ Dateien vor Manipulation und Missbrauch schützen

Nach dem Studium dieses Kapitels werden Sie verstehen, dass allzu sorgloser Umgang mit dem Computer und dem Internet große Gefahren birgt. Andererseits wird erklärt, dass Sie bei Einhaltung bestimmter Sicherheitsstandards und Richtlinien keine Angst vor dem Anwenden moderner Computertechnologie haben müssen.

1.1. Daten und Informationen

Sie kennen sicher die Begriffe **Daten** und **Datenverarbeitung**. Auch **Informationen**, **Informatik** und vielleicht sogar die so genannte **Informationsgesellschaft** sind für Sie keine Fremdwörter. Aber haben Sie sich schon einmal den Kopf zerbrochen über die eigentliche Bedeutung dieser Begriffe?

1.1.1. EINE ETWAS ANDERE DEFINITION VON DATEN UND INFORMATIONEN

Hier werden Daten ganz bewusst sehr allgemein definiert, um zu verdeutlichen, dass Daten und Informationen nicht erst seit der Erfindung des Computers bedeutsam sind.

Daten

Daten sind nichts anderes als die Codierung von Materie und der aus den Daseinsformen der Materie abgeleiteten Informationen, die im codierten Zustand jeden Informationsgehalt verloren haben. Es stellt sich auch die Frage, ob es überhaupt eine absichtslose und zufällige Codierung gibt. Ist es etwa vorstellbar, dass die in den Zellkernen enthaltenen genetischen Informationen zufällig so angeordnet sind, dass sie nachfolgend durch Dekodierung und Datenauslesen per Überführung in Eiweißstoffe jenen Informationsgehalt gewinnen, der solch komplexe Zellverbände entstehen lässt, die schließlich auch die Körper von Pflanzen und Lebewesen bilden?



Daten sind eine Ansammlung von Einsen und Nullen

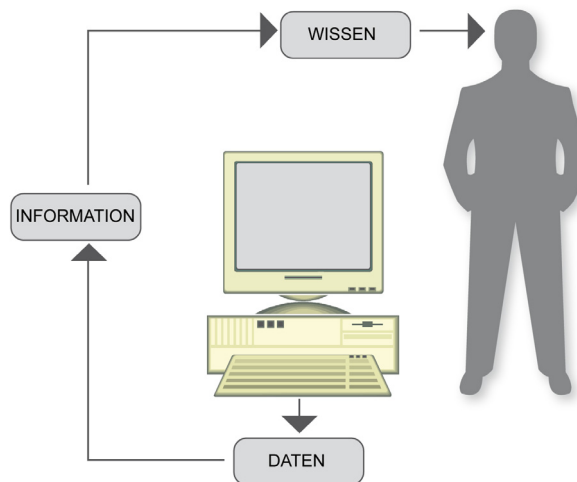
Auch dieses Lehrbuch wurde mittels Computer geschrieben. Wie groß ist die Wahrscheinlichkeit, dass die diese Texte codierenden Nullen und Einsen, welche sich auf mehr als eine Million belaufen, im Hintergrund zufällig so angeordnet wurden, dass sie diesen Text ergeben?

Mit Bezug auf den Computer sind Daten in letzter Konsequenz jene Ansammlungen von zwei Zuständen - gekennzeichnet durch 0 und 1 -, die die in der „analogen Welt“ vorhandenen vielfältigen Informationen codieren. Natürlich müssen Programme dieses Codieren übernehmen. Der Verlust von Programmen, die ein Dekodieren solcher binärer Daten ermöglichen, würde die Daten nahezu unlesbar machen und der Informationsgehalt als solcher würde verloren gehen. Ebenso verhält es sich mit verschlüsselten Daten. Der Verlust des Schlüssels macht die Daten unlesbar. (Lesen Sie dazu mehr im Abschnitt „ Schutz von vertraulicher Information“.)

Informationen

Wir erkennen jedenfalls, dass z. B. der Bauplan des menschlichen Körpers in seinem Genom gespeichert ist und z. B. in seinen Kindern wieder Informationsgehalt gewinnt.

Es gibt aber auch codierte Daten, die erst durch die Interpretation eines zur Kommunikation befähigten Lebewesens - wie z. B. den Menschen - aus diesen Daten wieder Informationen für andere Menschen entstehen lassen. Ob allerdings diese Daten richtig interpretiert werden, ist ein Kapitel für sich.



Aus Daten entsteht über Information Wissen

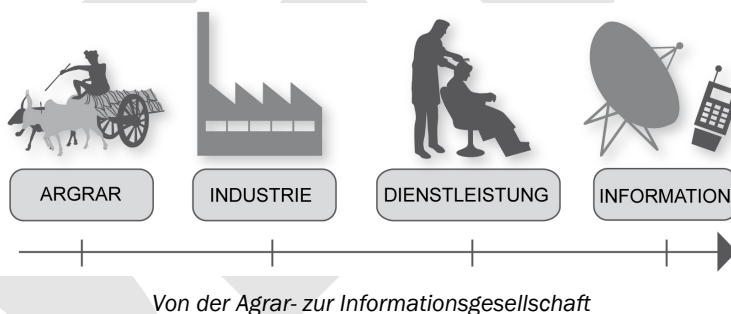
Ein simples Beispiel soll diese Angaben verdeutlichen: Wir wissen heute, dass sich die Erde um die Sonne dreht. Vor noch nicht allzu langer Zeit betrachtete der Mensch die Erde als Mittelpunkt des Universums. Welches Tier interessiert es, ob sich die Sonne um die Erde oder die Erde um die Sonne dreht? Nur jenes Tier, das über solche Beobachtungen mit anderen Tieren kommunizieren möchte und aus diesen Beobachtungen Schlussfolgerungen mit weitreichender Konsequenz zieht: der Mensch.

Je entwickelter und kreativer die Informationen interpretiert werden, desto „menschlicher“ werden sie. Je umfangreicher und wertvoller die interpretierte Information für die Menschheit ist, umso wichtiger wird es, über Systeme zur absolut sicheren Weitergabe des Wissens an nachfolgende Generationen zu verfügen.

Die naturwissenschaftlich gewonnenen Erkenntnisse explodieren. Denken Sie in diesem Zusammenhang etwa an die Datenflut, welche nach Versuchen im Teilchenbeschleuniger CERN anfallen. Das Auswerten dieser Daten kann nur mehr mit besonders leistungsfähigen Computersystemen erfolgen, die uns in letzter Konsequenz helfen, die in allem innewohnende Logik zu erkennen.

1.1.2. INFORMATIONSGESELLSCHAFT

Bei dieser Gesellschaftsform handelt es sich um jene, die auf die aktuelle Dienstleistungsgesellschaft und Informationstechnologiegesellschaft folgen wird. Mit dem Sesshaft werden entstand einst die Agrargesellschaft, in der die meisten Menschen mit Ackerbau und Viehzucht beschäftigt waren. Darauf folgte die Industriegesellschaft, die den meisten Menschen in Fabriken Arbeit bot. Heutzutage ist nahezu jeder Bürger beruflich Dienstleister. Die Informationstechnologiegesellschaft zeichnet sich dadurch aus, dass alles, was mit Computern und Massenkommunikationssystemen - wie z. B. Mobilfunk - zusammenhängt, viele neue Arbeitsplätze schafft.



Allmählich übernehmen Computersteuerung und Roboter immer mehr Arbeit, für die nur geringe bis mäßige Qualifikation erforderlich ist. Vor allem automatisierbare Arbeitsabläufe werden Computern, Robotern und automatisierten Produktionsstraßen überantwortet. Die Zeit ist nicht mehr fern, in der in unseren Wohnungen rund um die Uhr insektenartige Flugobjekte permanent herumschwirren werden, um jedes Staubkrümelchen aufzusaugen.

Allmählich verliert herkömmliche Dienstleistungsarbeit sukzessive an Bedeutung, da diese in weiten Bereichen durch Computersteuerung und Roboter ersetzt werden kann. Und derart erreichen wir Schritt für Schritt die Informationsgesellschaft, die wie folgt definiert werden kann:

Das kreative Humankapital ist der wichtigste Produktivitätsfaktor in der Informationsgesellschaft.



Der Computer kann sehr viel – und er kann aufgrund der immer rascher funktionierenden Prozessoren und Speicher, die zudem immer kleiner dimensioniert werden, immer mehr. Aber er kann eines nicht – und wird es auch nie können:



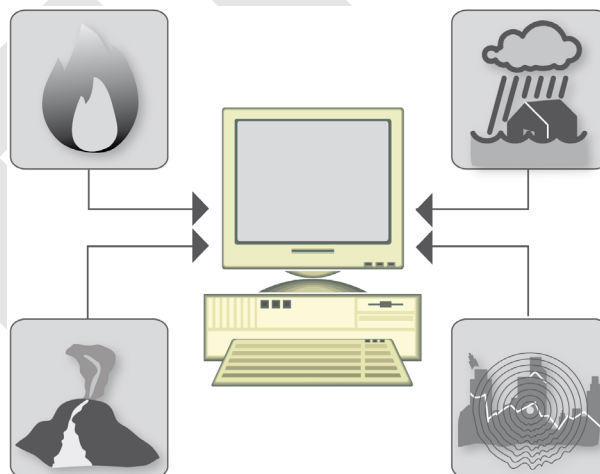
Der Computer ist nicht kreativ.

Computer und Roboter können nur das ausführen, was die Software, was die Programme vorgeben. Und diese Programme wurden von intelligenten Menschen mit hohem Kreativpotential entwickelt. Es ist vollkommen ausgeschlossen, dass Computer oder vernetzte Computersysteme jemals die Herrschaft über den Menschen übernehmen können, solange der Mensch nicht Software entwickelt, die eine derartige Unterwerfung ermöglicht.

Es erscheint zum Beispiel zwingend logisch, dass computergesteuerte Maschinen Möbelteile zehntelmillimetergenau aus Holz schneiden und fräsen. Aber ist es vernünftig, so etwas zu fördern und daneben die erfüllende Bindung von Kreativität an handwerkliche Geschicklichkeit zu eliminieren?

1.2. Datenzerstörung und Datenmissbrauch

Daten sind prinzipiell bedroht durch Einwirkung so genannter **höherer Gewalt**. Naturkatastrophen wie z. B. **Erdbeben, Vulkanausbrüche, Hochwasser, Meteoriteneinschläge** und **Feuer** können Hardware und die in den Speichermedien abgelegten Daten schlagartig zerstören.



Bedrohungsszenarien

Physisches Zerstören von Computern und Computernetzwerken als Folge kriegerischer Handlungen oder Einschleusung von **Computerviren** mit Schädigung bis kompletter Zerstörung von Daten sollen den Angegriffenen in seiner Handlungsfähigkeit so weit einschränken, dass er als Geschwächter zu einer leichten Beute wird.

Jedoch ist das bewusste Zerstören von Daten des Gegners weitaus weniger intelligent als die Daten des Angegriffenen nach Einschleusung von vielfältigen Schadensprogrammen auszuspionieren, zu manipulieren und missbräuchlich zu verwenden.

„Gelegenheit macht Diebe“ ist auch im Zusammenhang mit unachtsamem Umgang mit Daten ein passender Ausspruch. Mitarbeiter einer Firma sind vertraglich - z. B. im Zuge eines Dienstvertrages - zur Geheimhaltung firmeninterner Daten zu verpflichten.

Es ist kein Kavaliersdelikt, ungefragt die Adressen von Kollegen auf einen USB-Stick zu kopieren und diese in weiterer Folge vielleicht sogar an Dritte weiterzugeben.



Vorsicht ist auch geboten bei Auftragsdatenverarbeitung, bei welcher das Auslagern von Datenverarbeitungsprozessen an externe Dienstleister erfolgt.

Sämtliche Datenträger, sowohl jene im Computergehäuse eingebauten als auch externe „Backup“(Sicherungskopie)-Medien, sind verschlossen aufzubewahren.

Der Zugriff auf einen Computer, auf welchem sich sensible Daten befinden, darf nur mit Benutzernamen und Kennwort erfolgen.



1.3. Cybercrime (Internetkriminalität)

Als Cybercrime wird jene Kriminalität bezeichnet, die sich der Techniken des Internets bedient. Wenn nur der Computer ohne Internetzugang bei der Begehung von Straftaten eine Rolle spielt, spricht man von **Computerkriminalität**. Diese Kriminalitätsformen nehmen quantitativ dramatisch zu.



virtueller Zugriff und realer Schaden

Das Internet hat in den letzten knapp 20 Jahren weltweit grundlegende Veränderungen hinsichtlich der Vernetzung von Wissen und Gedankenaustausch ermöglicht und multiethnische Verflechtungen motiviert, wie sie zuvor undenkbar schienen. Zweifellos stellen das Internet und seine wichtigen Dienste

- E-Mail
- WWW (World Wide Web)
- Newsgroups (Gesprächsforen)
- Chatrooms
- Social Networking Websites

u. a. großartige Möglichkeiten des Informationstransports dar, der jedoch auch große Gefahren birgt.

1.3.1. VON PERSONEN AUSGEHENDE GEFAHREN

Kriminelle Personen erkennen die Chance, ihre auf Gewinn abzielenden Methoden über die Kommunikationsmöglichkeiten des Internets abzuwickeln:

- ! Vom Computerbenutzer unbemerkt, wird Malware (Schaden verursachende Software) installiert, die dann auf vielfältige Art und Weise wirken kann.
- ! Das unautorisierte Anbieten gecrackter Software schädigt Softwarehersteller.
- ! Illegale Pornographie („Kinderpornographie“) zerstört Existenzen.
- ! Das Vertrauen von arglosen Bürgern wird erschlichen und folgend ausgenützt, um z. B. Geldtransaktionen mittels erschlichener TAN-Nummern (Transaktionsnummern) auf illegale Konten vornehmen zu können.
- ! Über Soziale Netzwerke kann nicht nur ein virtueller, sondern auch, in weiterer Folge, ein realer Zugriff auf Opfer erfolgen.

1.3.2. STRAFTATBESTÄNDE VON INTERNETKRIMINALITÄT

Das Fundament zur Erfassung von Internetkriminalität bilden drei Straftatbestände, die allgemein in die Strafgesetzbücher aufgenommen wurden:

Ausspähen von Daten

Strafbar macht sich, wer nicht für sich bestimmte und gegen unberechtigten Zugang besonders gesicherte Daten sich oder einem anderen verschafft.

Dabei wird diskutiert, welche Daten besonders schutzwürdig sind; persönliche, „wertlose“ Daten oder aber Daten, die einen ideellen oder wirtschaftlichen Wert haben.

Datenveränderung

Der Datenveränderung macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Auch der Versuch ist strafbar.

Computersabotage

Der Computersabotage macht sich strafbar, wer eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert.

Durch derartige Handlungen können Privatpersonen, Betriebe, Unternehmen oder Behörden maßgeblichen Schaden erleiden.

1.3.3. MISSBRAUCHSFORMEN DER INTERNETKRIMINALITÄT

Verbreitung von gegen nationale Gesetze verstoßendem politisch-extremistischem Material, Verbreitung von kinderpornographischem Material, ...

- Manipulation von Hyperlinks,
- unbefugtes Lesen von E-Mails,
- diverse Methoden zum Zwecke der Datensabotage und -spionage.

Unter dem Begriff der „**Multimedialen Kriminalität**“ wird „jede gesetzeswidrige und/ oder ethisch verwerfliche Handlung im Zusammenhang mit dem Missbrauch der neuen Kommunikationstechniken und Medien, die weitgehend von sozial unauffälligen Tätern durchgeführt wird und in ihrer Begehung völlig anonym geschieht“ subsumiert.¹



1.3.4. HACKING

Als Hacking bezeichnet man den Zugriff auf ein Computernetz, der ohne Wissen des „Ge-hackten“ erfolgt. Der Hacker setzt sich dabei über verschiedene Sicherheitsvorkehrungen jenes Systems hinweg, in das er eindringt.



Hacker versuchen in ein Computersystem einzudringen

Hacker sind prinzipiell an den Grundlagen von Betriebssystemen interessierte Menschen, die beständig bemüht sind, Sicherheitslücken zu finden, um über diese in Computer einzudringen und in weiterer Folge an persönliche Daten zu gelangen.

Ethisches Hacking

Ethisches Hacken ist gesetzlich legitimiert. Manche Firmen beauftragen Hacker, damit jene ganz bewusst und gezielt Sicherheitslücken aufspüren, um diese zur Abwehr von nicht vorhersehbaren Hack-Angriffen schließen zu können.

Cracking

Eine Analyse von Computerprogrammen zum Zwecke der Kopierschutzentfernung wird als „Cracking“ bezeichnet. Leute, die sich mit Cracking beschäftigen, nennt man **Cracker**.

Ein **Crack** kann zum einen die Kopie eines Programms sein, von dem der Kopierschutz entfernt wurde, zum anderen das Programm selber, mit dessen Hilfe der Kopierschutz bei anderen Programmen entfernt wird.

¹ Definition entnommen aus Vassilaki, Multimediale Kriminalität

1.4. Schutz von personenbezogenen Daten

Personenbezogene Daten sind

- ethnische Abstammung (laut Datenschutzgesetz besonders schutzwürdig)
- Name
- Adressen (sowohl IRL als auch E-Mail)

Tipp

IRL steht für **in real life** und kennzeichnet den momentanen geographischen Aufenthaltsort der Biomasse Mensch.

- Sozialversicherungsnummer
- Glaubenszugehörigkeit
- politische Ausrichtung
- sexuelle Orientierung
- Krankengeschichte
- Leumundszeugnis,
- Vorstrafenregister
- Insolvenzdaten.



Vorsicht: Überwachung!

Sie haben sicher erkannt, dass derartige Daten nicht absolut, unter allen Umständen und für alle Personen gleich behandelt werden können und müssen. Was ein Mensch freiwillig über sich preisgibt, sollte statthaft sein. Jedoch gibt es auch dabei Grenzen, die anhand des folgenden Beispiels erklärbar sind: Ihre Sozialversicherungsnummer darf nur von Ihnen und nicht auch von Fremden zur eventuell kostenintensiven Behandlung deren Krankheiten verwendet werden. In diesem Fall hat auch die Allgemeinheit ein Interesse daran, dass Ihre persönlichen Daten nicht von Dritten verwendet werden, weil ja die Allgemeinheit die Kosten von Behandlungen trägt.

1.4.1. DATENSCHUTZ

Jede Person hat prinzipiell das Recht, über die Weitergabe ihrer personenbezogenen Daten selber zu bestimmen. Es wird auch vom Recht auf **informationelle Selbstbestimmung** gesprochen. Mittels Datenschutz soll der so genannte **gläserne Mensch** verhindert werden.

Die rasante Entwicklung des Computers hat dazu geführt, dass die persönlichen Daten immer leichter und schneller aufgenommen, verarbeitet, weitergegeben und analysiert werden können. Neue Methoden der Datenerfassung ergeben sich per WWW, E-Mail, Mobilfunk, Videoüberwachung und elektronische Zahlungsmethoden.

Tipp

Sowohl staatliche Stellen als auch Firmen und Einzelpersonen haben Interesse an personenbezogenen Daten.

Folgende Umstände sind dabei von besonderer Bedeutung:

- ! **Rasterfahndung und Telekommunikationsüberwachung** zwecks Verbrechensbekämpfung (ein Beispiel ist die **Section Control**, mit der die Einhaltung einer vorgeschriebenen Höchstgeschwindigkeit überwacht wird und zu deren Zweck die Nummernschilder bei der Ein- und Ausfahrt in bzw. aus einem bestimmten Streckenabschnitt erfasst werden; die Daten von Fahrzeugen, deren Lenker die Geschwindigkeitsbeschränkungen beachtet haben, sind unmittelbar nach deren Aufnahme wieder zu vernichten.)
- ! **Auswertung von Finanztransaktionsdaten** zwecks Aufklärung von Steuerdelikten durch Finanzbehörden.
- ! **Mitarbeiterüberwachung** zur Effizienzsteigerung in Behörden und Betrieben.
- ! **Kundenprofile** haben strategische Bedeutung für künftigen Einsatz von gezielter Werbung und Produktentwicklung.

Leider erkennen weite Bevölkerungskreise nach wie vor nicht die faktische Bedeutung derartiger Daten, weshalb mit deren Preisgabe auch äußerst fahrlässig umgegangen wird.

Anhand eines Beispiels soll erklärt werden, welche Bedeutung Ortungsdaten von Handys für ein Reisebüro haben könnten:

Wenn sämtliche angemeldete Handys über einen Zeitraum von einigen Jahren täglich geortet und die Daten ausgewertet würden, könnten von den Aufenthaltsorten der Handys über Rückschlüsse auf die Urlaubsziele der Handybesitzer gezielte Urlaubsangebote unterbreitet werden. Die Kosten einer breitflächigen Werbung mit einer sehr geringen Trefferquote würden damit dramatisch reduziert. Jedoch: Wollen Sie, dass jeder Fremde über Ihre Urlaubsvorlieben Bescheid weiß? Was könnte geschehen, wenn solche Daten von Kriminellen gehackt würden - und in weiterer Folge Diebsbanden gezielt die Wohnungen und Häuser ihrer Opfer aufsuchen, weil sie „mitlesen“, wo sich gerade deren Handys befinden?

1.4.2. BEDEUTUNG DES INTERNETS IM ZUSAMMENHANG MIT DATENSCHUTZ

Was nützen die besten EU-Richtlinien und nationalstaatlichen Gesetze zum Datenschutz, wenn krimineller Datenklau und Datenmissbrauch nicht praktisch verfolgbar ist, weil sich die Täter in Staaten aufhalten, in denen keine derartigen Datenschutzgesetze verabschiedet wurden? Datenschützer müssen sich somit auch um die effektive Durchsetzbarkeit der Datenschutzrichtlinie kümmern.

In den USA ist der Datenschutz nur sehr sporadisch durch Gesetze oder Vorschriften geregelt. Es gibt auch keine rechtlichen Regelungen bezüglich der Aufbewahrungsdauer gesammelter personenbezogener Daten. Des Weiteren gibt es auch keine Verpflichtung für Behörden oder Unternehmen, Auskunft darüber zu erteilen, welche persönlichen Daten gespeichert wurden (ausgenommen ist nur der „Freedom of Information Act“) und auch keine Verpflichtung, falsche Daten korrigieren zu müssen.

Die europäische Datenschutzkonvention wurde 1981 durch den Europarat verabschiedet, ist heute nach wie vor gültig, hat jedoch nur empfehlenden Charakter.

1.4.3. DATENSCHUTZRICHTLINIE

Die **Richtlinie 95/46/EG** (Datenschutzrichtlinie) ist für Mitgliedsstaaten der Europäischen Union bindend und muss von jenen mittels nationalstaatlicher Datenschutzgesetze umge-

setzt werden. Diese Richtlinie gilt jedoch nicht im Zusammenhang mit Legislative (gemeinsame Außen- und Sicherheitspolitik) und Exekutive (polizeiliche und justizielle Zusammenarbeit), also bei der so genannten Dritten Säule der Union.



Datenschutzrichtlinien der EU

Aus der Richtlinie ergeben sich Mindeststandards für den Datenschutz. Sie verbietet im Regelfall die Verarbeitung sensibler personenbezogener Daten (wie z. B. jene der ethnischen Herkunft). Ausnahmen von dem Verbot bestehen jedoch, wenn die jeweils betroffene Person ausdrücklich der Verarbeitung der freiwillig angegebenen persönlichen Daten zugestimmt hat, oder zugunsten arbeitsrechtlicher Bestimmungen und bei „wichtigem öffentlichem Interesse“.

Die wichtigsten Prinzipien des Datenschutzes sind:

- ! Datensparsamkeit und Datenvermeidung
- ! Erforderlichkeit
- ! Zweckbindung

Die aus Datenschutzgesetzen resultierenden wichtigsten Folgen sind:

- ! Die aufgenommenen Daten dürfen nicht an Dritte weitergegeben werden.
- ! Jeder hat das Recht auf Einsichtnahme der über ihn gespeicherten Daten.
- ! Jeder hat das Recht, unrichtig aufgenommene Daten korrigieren zu lassen.

Zu Letzterem ein Beispiel:

Sie kommen zufällig zu einer nicht angemeldeten Demonstration radikaler politischer Kreise. Die Polizei nimmt auch Ihre Personalien auf. Sie vermuten, dass Sie nun als „Rechtsradikaler“ oder „Linksradikaler“ in den elektronischen Akten des Innenministeriums geführt werden, verlangen daher, die Daten einsehen zu können und, in weiterer Folge, dass diese unrichtig aufgenommenen Daten gelöscht werden.

1.4.4. MAßNAHMEN UND RICHTLINIEN ZUM DATENSCHUTZ

Beachten Sie folgende Schutzmaßnahmen und Richtlinien:

Persönliche Daten nur in unbedingt notwendigem Maß bekannt geben

Was nützen die besten Gesetze, wenn die Menschen nicht erkennen, wie wichtig es ist, sorgsam mit den eigenen Daten und den Daten jener Firmen, bei denen sie arbeiten, umzugehen. Bereits jetzt schon kommen die Gerichte kräftig ins Schwitzen, wenn es um Urteilungen von Verstößen gegen das Datenschutzgesetz geht.

Ein Grund dafür ist, dass die Daten förmlich auf den „virtuellen Straßen des Internets“ oder in ungeschützten oder ungenügend geschützten PCs „zur freien Entnahme“ herumliegen?

Folgende Fragen sollen Sie zum Nachdenken anregen:

- Warum werden die realen Geldbörsen aufgrund von zahlreichen Kundenkarten, über die Verbrauchergewohnheiten personalisiert abgespeichert werden können, immer dicker?
- Bei wie vielen Preisausschreiben haben Sie bereits der elektronischen Verarbeitung Ihrer Daten zugestimmt?

Lesen Sie bei der Weitergabe Ihrer Daten auch immer das Kleingedruckte. Meist gibt es einen Hinweis, in dem steht, dass Sie auch der Weitergabe Ihrer Daten an Dritte zustimmen.

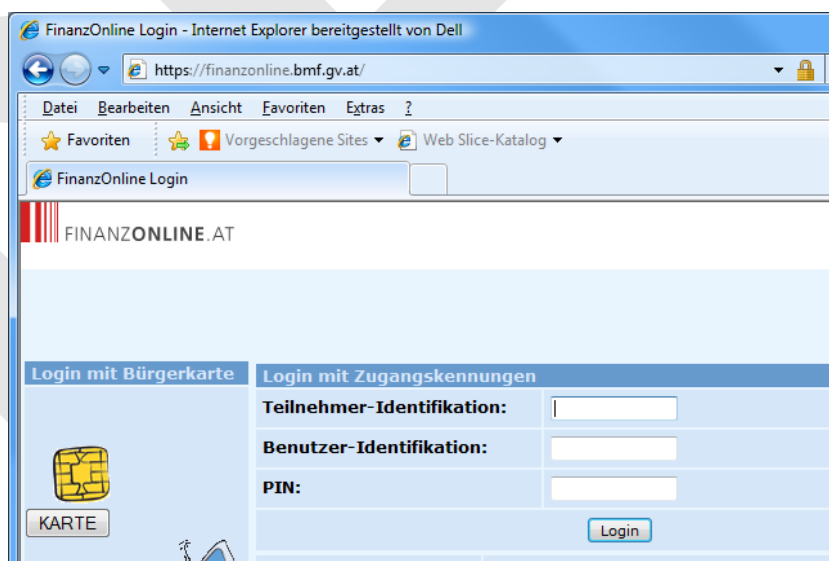
Tipp

Passwörter (Kennwörter)

Das **Intranet** ist das Computernetz einer Firma oder einer Behörde (eines Amtes), das im Regelfall sehr gut geschützt ist gegenüber Hacker-Angriffen. Aber selbst derartige Netze großer Firmen (auch von Banken) wurden bereits erfolgreich gehackt - mit nicht absehbaren Schadensfolgen, wie sie sich z. B. aus missbräuchlicher Verwendung von Kundendaten ergeben können.

Das **Extranet** ist jener Teil eines Intranets, der auch für Kunden zugänglich ist. Der Zugang zu einem Extranet darf nur mit **Benutzernamen** und **Kennwort** erfolgen. Beispiele für derartige Extranets sind etwa jene des Finanzamts oder einer Bank.

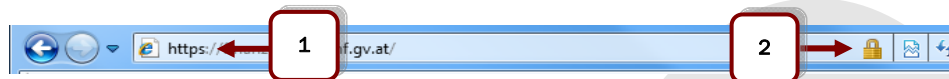
Banken bieten ihren Kunden die Möglichkeit, das eigene Konto per Internet einzusehen und auch Geldgeschäfte (z. B. Überweisungen) online durchzuführen. Allerdings müssen derartige Finanztransaktionen stets durch die abschließende Eingabe einer **TAN-Nummer** (**T**ransa**k**tions**n**ummer) abgeschlossen werden.



Zugang zu FinanzOnline

HTTPS

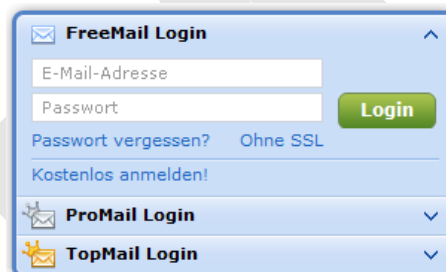
Selbstverständlich dürfen alle Geldgeschäfte, auch alle Zahlungen, mittels Kreditkarte, im Internet nur über ein sicheres Datenübertragungsprotokoll abgewickelt werden, mit dessen Hilfe die Daten verschlüsselt gesendet werden. Dieses Datenübertragungsprotokoll ist das **HTTPS (Hypertext Transfer Protocol Secure)**. Die sichere Datenübertragung erkennen Sie in der Adressleiste Ihres Browsers am vorangestellten Protokoll **https** (1) und zumeist auch an einem **Schloss – Symbol** (2).



Übertragungsprotokoll in der Adressleiste und Schloss-Symbol

E-Mail

Der Zugang zu webbasierten E-Mail-Diensten (wie z. B. GMX, Hotmail, Google-Mail,...) muss stets über ein Passwort erfolgen. Auch die Nutzung aller Online-Dienste, die diverse Firmen anbieten (wie z. B. Mobilfunkunternehmen) darf nur nach Eingabe eines Kennworts möglich sein.



Zugang zu einem webbasiertem E-Mail-Dienst

Passwortschutz und Computer

Tipp

Die meisten Computer bieten die Möglichkeit, im BIOS (basic input output system) das Booten (Hochfahren) des Rechners durch ein Passwort zu schützen. Dieser Schutz ist jedoch nicht sehr zuverlässig und nur als eine Art „Kindersicherung“ anzusehen, da er durch ein vom Hersteller des BIOS vorgegebenes Masterpasswort umgangen werden kann.

Bei so genannten Windows-Rechnern, bei denen die Betriebssysteme Vista oder Windows7 installiert sind, sollten die Zugriffe zu den jeweiligen Benutzern durch Passwörter geschützt werden, da bei diesen Betriebssystemen der Zugriff zu jenen Dateien, die sich in einem vom Benutzerordner ausgehenden Ordner befinden, für andere Benutzer gesperrt ist.

Tipp

Allerdings ist auch dieser Schutz nicht wirklich geeignet, größere Datenmengen zu schützen, da die Verwaltung komplexerer persönlicher Daten aus Gründen der Transparenz NICHT in den vom Betriebssystem vorgeschlagenen Ordnern erfolgen sollte.

Zum Schutz persönlicher Daten in Dateien eignet sich jedoch das **Verschlüsseln** von Dateien wesentlich besser. Lesen Sie dazu mehr im Abschnitt „Sichere Dateien“.

1.4.5. DATENSICHERHEITSMERKMALE

Folgende drei Datensicherheitsmerkmale sind bedeutsam:

Vertraulichkeit

Informationen müssen vor unbefugter Preisgabe geschützt sein. Eine Nachricht ist nur für einen beschränkten Empfängerkreis vorgesehen.

Integrität

Integre Daten sind über einen bestimmten Zeitraum hinweg vollständig und unverändert geblieben. Integrität bietet Schutz vor fehlerhafter Datenübertragung und vor vorsätzlicher Veränderung.

Verfügbarkeit

Per Computer und Internet zur Verfügung gestellte Dienste müssen mit Ausnahme der erlaubten Ausfallszeit verfügbar sein. Eine Verfügbarkeit ist auch dann nicht mehr gegeben, wenn die Antwortzeit eines Systems eine gewisse Kenngröße überschreitet.

Denken Sie an die ärgerlichen Ausfälle einer EC-Card (Bankomat)-Zahlung, die mittlerweile immer seltener auftreten.

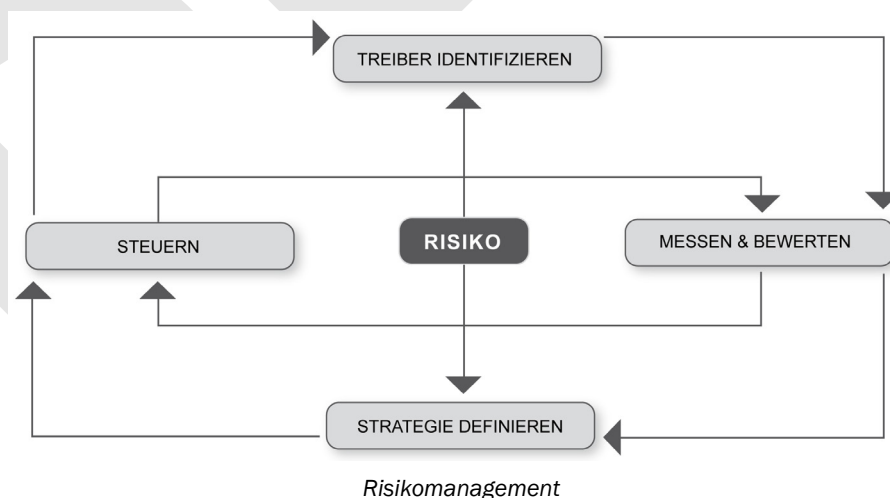


1.4.6. SICHERHEITSTRATEGIEN UND RICHTLINIEN

In der **Informations- und Kommunikationstechnologie (IKT)**, die das Zusammenwirken der Digitaltechnik sowohl bei der Informationsverarbeitung als auch bei der Informationsweitergabe kennzeichnet, ist es von großer Bedeutung, dass Sicherheitsstrategien und Richtlinien erstellt und von den involvierten Personen eingehalten werden müssen:

Risiko Management

- **Betriebliches Kontinuitätsmanagement:**
In der Betriebswirtschaftslehre wird darunter die Entwicklung von Strategien, Plänen und Handlungen verstanden, um Tätigkeiten oder Prozesse, deren Unterbrechung der Organisation ernsthafte Schäden oder vernichtende Verluste zufügen würden, zu schützen bzw. alternative Abläufe zu ermöglichen.



- **Notfallwiederherstellung (auch Disaster Recovery):**
setzt ein, wenn nach einem Unglück Datenwiederherstellung notwendig wird und Infrastruktur, Hardware und Organisation ersetzt werden müssen.

- **Information Security Management System (ISMS) :**
Es gibt bestimmte Verfahren und Regeln in einem Unternehmen, die notwendig sind, um Informationssicherheit zu definieren und einer Steuerung, Kontrolle, Aufrechterhaltung und fortlaufenden Verbesserung zuzuführen.

Unternehmensbezogene Sicherheitsarchitektur

Es werden Ziele, Rollen und Verantwortlichkeiten definiert. Dabei spricht man von so genannten Policies die folgendes beinhalten:

- Password-Richtlinien
- E-Mail-Richtlinien
- Firewall-Richtlinien
- Server-Richtlinien
- Überprüfung von Sicherheitsstrategien
- Anwendung zyklischer Security Audits

Verschlüsselungsverfahren

Z. B. **PKI (Public-Key-Infrastruktur)**: Mit diesem System können digitale Zertifikate ausgestellt, verteilt und geprüft werden. Damit kann vernetzte Kommunikation abgesichert werden.

Biometrische Verfahren

Zugang zu realen Räumen und Computern mittels Fingerabdruck, Iris-Kontrolle.

Auswahl geeigneter Dienstleister, Outsourcing-Nehmer und Sicherheitsberater

1.5. Social Engineering

Social Engineering verfolgt den Zweck, unbefugt an fremde Daten zu gelangen. Und bekanntlich heiligt der Zweck alle Mittel: In diesem Fall ist das Mittel die zwischenmenschliche Manipulation.

1.5.1. FORMEN DES SOCIAL ENGINEERING

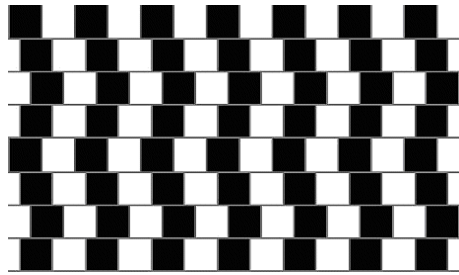
Manipulative Telefonanrufe

Zum besseren Verständnis ein Paradebeispiel:

Ein so genannter **Social Engineer**, der widerrechtlich an geschützte Daten gelangen möchte, informiert sich auf verschiedene Art und Weise über jenes Unternehmen, von welchem er die gewünschten Daten erlangen möchte.

Diese Informationen erhält er z. B. über diverse Anrufe bei Mitarbeitern dieser Firma, wobei er mit wechselnden Identitäten auftreten kann. Aus den zusammen getragenen Informationen entwickelt er eine Strategie, mit der es gelingen soll, Mitarbeiter bei folgenden Anrufen so weit zu manipulieren, dass diese glauben, dass es jenen Haustechniker, als der sich der Social Engineer schließlich ausgibt, tatsächlich gibt.

Und dann ist es nicht mehr weit, bis man diesem lieben, lustigen, umgänglichen Arbeitskollegen, der einen schon mal vorab auf ein Bier oder einen Kaffee eingeladen hat, so weit vertraut, dass man ihm Passwörter verrät, die dieser zufälligerweise vergessen hat, weil man nicht möchte, dass ihn der strenge Chef, den ohnehin keiner mag, dafür rügt, wenn er nochmals nachfragen muss.



Sie dachten, Sie seien nicht manipulierbar? Sehen Sie die geraden waagrechten Linien?

Es ist klar, dass derartiges Social Engineering bei großen Firmen mit vielen Mitarbeitern, die sich untereinander kaum oder mitunter gar nicht kennen, besser funktioniert als in einem Kleinbetrieb. Ein Social Engineer verfügt auch idealerweise über eine gute Menschenkenntnis und erkennt sehr schnell, ob sein Gegenüber ein misstrauischer oder leichtgläubiger Mensch ist.

Dumpster Diving

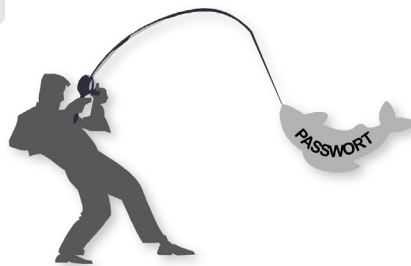
Eine spezielle Form der Informationsbeschaffung stellt das so genannte **Dumpster Diving** dar, bei welchem der Müll des potentiellen Opfers durchsucht wird, um derart dessen soziales Umfeld in Erfahrung zu bringen, was bei folgenden Anrufen dazu dienen kann, vertrauenswürdig zu erscheinen.

Der „Enkeltrick“

Beim so genannten **Enkeltrick** suchen Betrüger gezielt nach sehr alten Personen, die z. B. ihren Anruf mit „rate mal, wer da spricht...“ eröffnen, in der Hoffnung, dass als Antwort Namen genannt werden, die in weiterer Folge den Einstieg zur Lügengeschichte mit teurem Ende einleiten, indem z. B. um Geld für das unverschuldet in Not geratene Enkelkind gebeten wird. - Dieses Beispiel soll zeigen, dass es derartiges Social Engineering schon „zu Großmutterns Zeiten“ gab und keine Erfindung des Computerzeitalters ist.

Phishing

Der Begriff Phishing setzt sich aus Passwort und Fishing, eventuell sogar aus "Password harvesting fishing" (Passwort pflücken, fischen) zusammen. So täuschen etwa betrügerische E-Mails vor, von z. B. Banken versendet worden zu sein, die zum Zwecke eines Service Kontonummer inkl. TAN-Nummern des Kunden benötigen. Es werden auch Texte versendet, die hohe Dringlichkeit vortäuschen, um eine rasche und unbedachte Antwort des Opfers zu motivieren.



Die E-Mails sehen in der Aufmachung jenen der z. B. regulär von Banken versendeten sehr ähnlich, was das Vertrauen in die Echtheit des E-Mail-Inhalts erhöht.

Besonders gefährlich wird es, wenn die Phishing-Angriffe durch Installieren von Trojanischen Pferden auf dem Rechner des Opfers vorbereitet werden. Ein solches Malware-Schadensprogramm kann z. B. die Kommunikation zwischen Bank und Kunden abfangen und auf eine gefälschte Website umleiten. Das Opfer glaubt dann, sich auf einer sicheren Website seiner Bank anzumelden, gibt jedoch derart seine Kontonummer und seinen PIN-Code über die gefälschte Website den Betrügern bekannt.

Die Angriffsziele sind jedoch nicht nur die Zugangsdaten zu Banken, sondern auch jene zu Versand- und Auktionshäusern oder sogar zu Singlebörsen.

Shoulder Surfing

Beim Shoulder Surfing versucht ein Betrüger, dem Opfer bei der Eingabe von sensiblen Daten „über die Schulter“ (daher: shoulder) zu sehen und diese derart auszuspähen.

Tipp

Seien Sie vorsichtig, wenn Sie eine fremde Person in ein freundliches Gespräch verwickelt, während Sie vor dem Geldautomaten (Bankomaten) stehen oder im Internetcafe per Computer Geldgeschäfte abwickeln wollen.



Eine vierstellige PIN-Nummer ist leicht nachzuvollziehen. Und wenn Ihnen der Trickdieb auf Tuchfühlung näher kommt, werden Sie irgendwann mit Schrecken bemerken, dass Ihnen auch die EC-Card (Bankomatkarte) fehlt und möglicherweise ein nicht unbeträchtlicher Betrag von Ihrem Konto abgehoben wurde.

Sogar in den eigenen vier Wänden ist man nicht vor Shoulder Surfing sicher. Ungünstig nahe am Fenster positionierte Tastatur und Bildschirm ermöglichen nämlich das Datenspähnen per Teleskop.

1.5.2. SCHUTZ VOR MANIPULATIVEN TELEFONANRUFEN, PHISHING ODER SHOULDER SURFING

Der beste Schutz vor allen derartigen Angriffen ist die Prävention und allein schon die Tatsache, dass man sich dieser Gefahren bewusst ist.

- ! **Seien Sie lieber misstrauisch und fragen Sie gezielt nach, um Angreifer aus der Ruhe zu bringen.**

Lassen Sie sich am Telefon auf keine Diskussionen ein, auch dann nicht, wenn der Anrufer noch so glaubwürdig erscheint. Testen Sie die Glaubwürdigkeit, indem Sie z. B. Fragen nach NICHT vorhandenen Kollegen oder Kolleginnen stellen. Suggestieren Sie dem Anrufer, dass er diese Kollegen auf jeden Fall kennen müsse. Und wenn ein Betrüger dann meint, diese Kollegen ja „plötzlich“ doch zu kennen, haben Sie ihn überführt.

- ! **Schützen Sie Ihren Computer generell vor Malware-Angriffen.**

(Beachten Sie dazu die Hinweise im Kapitel „Malware“.) Beantworten Sie keine E-Mails, von deren Authentizität Sie nicht absolut überzeugt sein können. Beim leisen Verdacht erkundigen Sie sich lieber beim angeblichen Absender derartiger E-Mails, ob diese tatsächlich von ihm stammen.

- ! **Lassen Sie Fremde nie zu nahe an sich heran, wenn Sie sensible Daten in einen Computer eingeben oder sich vor einem Geldausgabeautomaten befinden.**

Scheuen Sie sich nicht, Fremde deutlich darum zu ersuchen, mehr Abstand von ihnen zu halten.

1.6. Identitätsmissbrauch

Es wird immer von **Identitätsdiebstahl** gesprochen. Jedoch ist die Bezeichnung **Identitätsmissbrauch** wesentlich zutreffender, weil einer Person ja nicht die Identität gestohlen, sondern diese nur von einer anderen Person angenommen wird, indem personenbezogene Daten missbräuchlich verwendet werden.



Identitätsmissbrauch einmal anders (gefunden bei Wikipedia)

Die Ziele eines Identitätsmissbrauchs sind, finanzielle Mittel vom Opfer abzuschöpfen oder den Ruf des Opfers zu schädigen.

Je mehr persönliche Daten vom Opfer bekannt sind, desto sicherer gelingt der Missbrauch: Name, Wohnadresse, Geburtsdaten, Sozialversicherungsnummer, Führerscheinnummer, Bankdaten (Kontonummer, Kreditkartennummer).

- Besonders häufige Formen von Identitätsmissbrauch sind **Betrug per Kreditkarten** und Plünderung von Konten.
- Neben finanziellen Nachteilen kann es besonders gefährlich werden, wenn der Betrüger **Straftaten im Namen des Betroffenen** begeht.
- Gefährdungen ergeben sich vor allem im Zusammenhang mit **E-Commerce**, wenn keine sicheren Identitätsfeststellungen vorgenommen werden. Derart kann es geschehen, dass eine Person Waren, die sie gar nicht erhalten hat, bezahlen soll, weil sie offiziell als Käufer gilt.
- Diverse webbasierte **soziale Plattformen** bieten ein großes Gefahrenpotential: Das Anlegen von Accounts bzw. Profilen im Namen einer Person, die davon gar nichts weiß, kann fatale Konsequenzen haben, wenn derart in weiterer Folge z. B. Verleumdungen durchgeführt werden. In diesem speziellen Fall ist sogar ein echter Identitätsdiebstahl möglich, weil derartige Plattformen für idente Daten nur eine Registrierung erlauben.

1.6.1. METHODEN DES IDENTITÄTSMISSBRAUCHS

Information Diving

Beim so genannten **Information Diving** wird z. B. auf Datenträgern von ausrangierten Computern nach verwertbaren geheimen oder vertraulichen Informationen gesucht. An diesem Umstand ist zu erkennen, wie wichtig eine absichtliche Datenvernichtung sein kann, wie sie im gleichnamigen Kapitel beschrieben wird.

Skimming

Beim **Skimming** werden von Magnetstreifen Daten ausgelesen und auf weitere Karten kopiert. Beispielsweise können derart EC-Card(Bankomatkarten)-Kopien missbräuchlich verwendet werden.

Das gleichzeitige Ausspähen von Magnetstreifendaten einer EC-Card zusammen mit der PIN an einem Geldautomaten (Bankomaten) führt in der Regel zur Kontoplünderung, nachdem nämlich die Daten der EC-Card auf einen leeren Kartenrohling kopiert wurden, wird dieser zur Bargeldbehebung verwendet.



Falsche Tastatur und falscher Kartenleser

Die Täter können z. B. direkt über dem Einschiesbeschacht ein kleines, kaum merkliches Kunststofflesegerät anbringen, das dann die Daten der EC-Card während des Einzugs in den Einschiesbeschacht zusätzlich ausliest. Gelegentlich werden solche zusätzlichen Lesegeräte bereits im Türöffner zur Bank angebracht, weil ja der Zutritt zu den Geldautomatenräumen meistens nur nach Einschieben der EC-Card möglich ist.

Oberhalb der Tastatur des Geldautomaten kann wiederum eine winzige Funk-Kamera, versteckt hinter einer Plastik-Leiste, angebracht sein, über welche die Täter die Eingabe des PIN-Codes filmen. Auch Tastenfeldattrappen, die täuschend echt wirken und über das eigentliche Tastenfeld geklebt werden, ermöglichen es, die Tastendrucke aufzuzeichnen.

Pretexting

Pretexting bezeichnet die Vortäuschung einer falschen Identität am Telefon, um an Daten anderer Personen zu gelangen. Derart besorgt sich eine kriminelle Person Informationen seines Opfers. Diese Informationen können z. B. sensible Daten sein, die in Rechnungen enthalten sind.

1.7. Sichere Dateien – ein Leitfaden

Sie selber können einiges dazu beitragen, dass Ihre Dateien sicher sind vor Zerstörung, missbräuchlicher Verwendung und Manipulation.

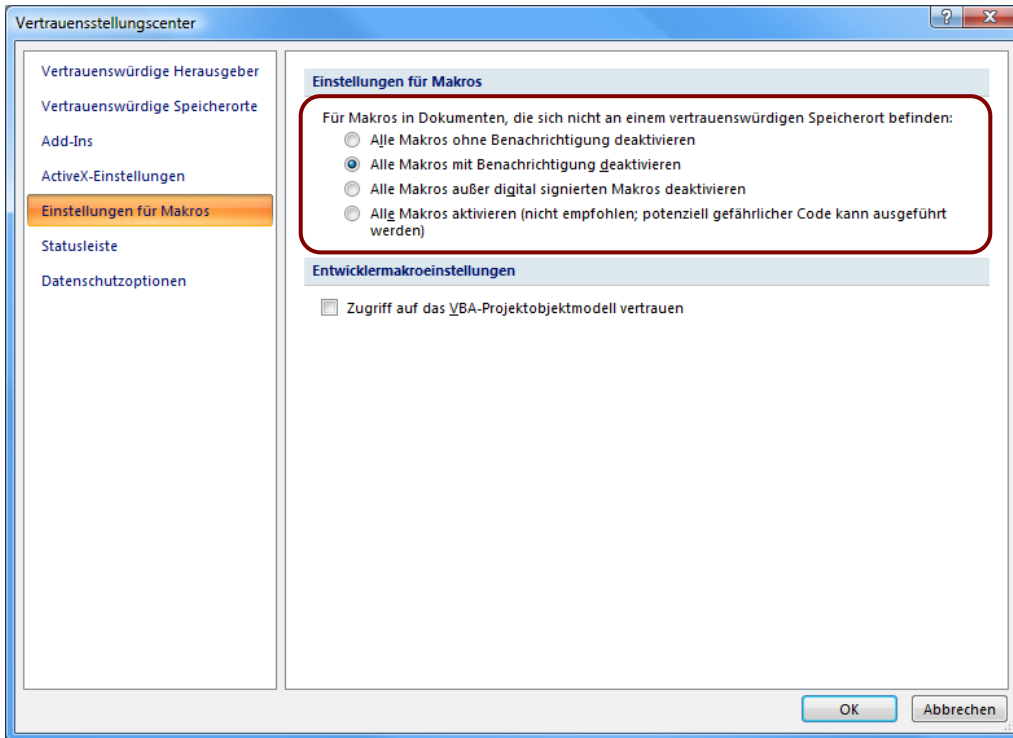
1.7.1. MAKRO-SICHERHEITSEINSTELLUNGEN

Ein **Makro** enthält Befehle und Aktionen, die ausgeführt werden, sobald das Makro aufgerufen wird. Derartige Makros werden in Anwendungsprogrammen zur Textverarbeitung und Tabellenkalkulation und in Datenbanken eingesetzt.

Ein **Makrovirus** nistet sich in Dokumente ein und ruft schädliche Funktionen auf. Es kann z. B. Texte in Word-Dateien verändern oder beliebige Dateien auf der Festplatte löschen.

Um vor solchen Makroviren Schutz zu bieten, können in den genannten Programmen Makro-Sicherheitseinstellungen aktiviert und den jeweiligen Bedürfnissen angepasst werden.

Beim Öffnen einer Datei, in der ein oder mehrere Makros enthalten sind, werden entsprechend der gewählten Sicherheitseinstellungen die Makros mit oder ohne Benachrichtigung deaktiviert, oder aber alle Makros außer der digital signierten deaktiviert.



Makrosicherheitseinstellungen

Die Einstellung, alle Makros automatisch zu aktivieren, ist nicht empfehlenswert.



Ein Schutz vor Makroviren ist dadurch gegeben, dass nur zertifizierte Makros von der jeweiligen Anwendung ausgeführt werden. Das ist vor allem für Behörden und größere Unternehmen interessant, bei denen Makros durch eine zentrale Zertifizierungsstelle überprüft und akzeptierte Makros zertifiziert werden.

1.7.2. PASSWORTSCHUTZ FÜR DATEIEN

Einen ganz speziellen Passwortschutz bieten viele Anwendungsprogramme.

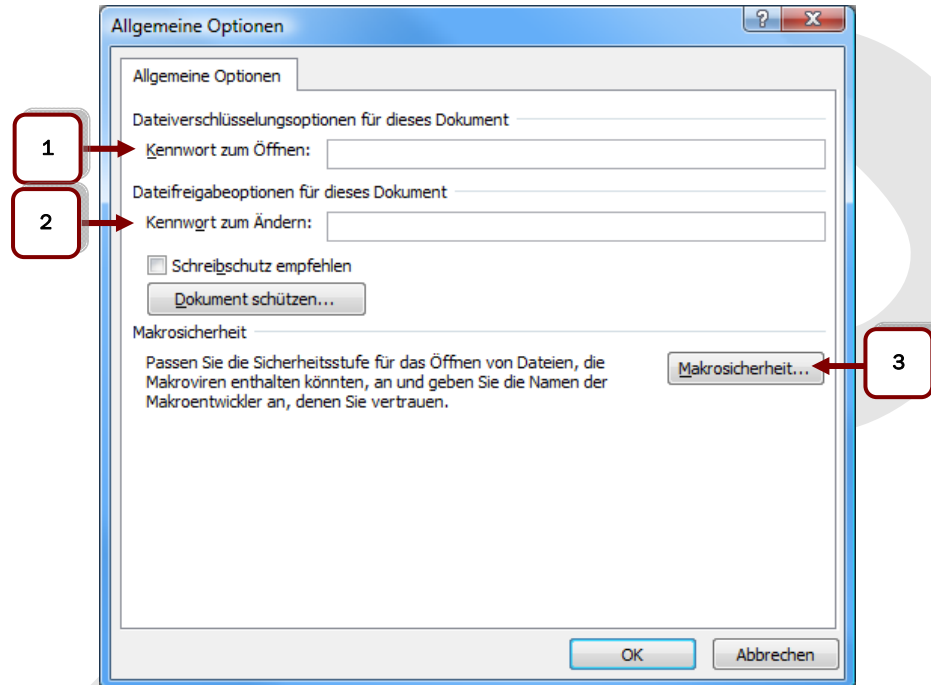
Über entsprechende Tools, die zumeist im Dialogfenster zum Speichervorgang zu finden sind, können Dateiverschlüsselungsoptionen in Verbindung mit Kennwörtern verwendet werden.

1. Ein **Kennwort zum Öffnen** der Datei ermöglicht in weiterer Folge das Öffnen der Datei nur jenen Personen, die dieses Kennwort kennen.

Vorsicht: Wenn Sie dieses Kennwort vergessen, ist auch für Sie diese Datei faktisch zerstört!



2. Ein **Kennwort zum Ändern** verhindert NICHT das spätere Öffnen und Lesen der Datei. Allerdings können Änderungen am Originaldokument im gleichen Ordner, aus dem es geöffnet wurde, unter dem gleichen Dateinamen nur mehr von denjenigen gespeichert werden, die das Kennwort zum Ändern im Zuge des Öffnens eingegeben haben. An dieser Datei vorgenommene Änderungen können jedoch sehr wohl unter einem anderen Namen gespeichert werden.



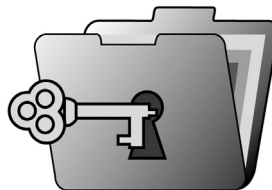
Die „Allgemeinen Optionen“ zum Festlegen von Kennwörtern in MS Word

3. Hier erhalten Sie auch die Möglichkeit, die Sicherheitsstufe für Dateien, die Makroviren enthalten könnten, anzupassen.

1.7.3. VERSCHLÜSSELUNG

Bei einer Verschlüsselung wird eine klar erkennbare Information ("Klartext", Bilder, Videos, Tondokumente) durch Verschlüsselung in eine unerkennbare Information verwandelt. Die derart uninterpretierbar gewordenen Daten können vom Empfänger (z. B. nach dem Senden im Internet) mittels Entschlüsselung wieder Informationsgehalt gewinnen.

- Bei **symmetrischen Verschlüsselungsmethoden** werden die gleichen geheimen Schlüssel für die Verschlüsselung und Entschlüsselung verwendet.
- Bei **asymmetrischen Verfahren** verwendet der Sender den **öffentlichen Schlüssel** des Empfängers und der Empfänger seinen **privaten Schlüssel** zur Entschlüsselung.



Verschlüsselung von Ordnern und Dateien

Eine Verschlüsselung kann jedoch auch dann erfolgen, wenn nicht an ein Senden der Daten gedacht wird. So ist es etwa möglich, unter Windows 7 mittels **EFS (encrypted file**

system) alle Ordner samt Inhalt zu verschlüsseln. Beim ersten Verschlüsseln wird für den jeweils angemeldeten Benutzer ein Zertifikat erstellt, welches mittels Kennwort geschützt werden kann.

Auch der Administrator des PCs kann dann nicht mehr auf die Dateien des Benutzers zugreifen.

Tipp

Der Schlüssel, der für die Dateiverschlüsselung verwendet wurde, sollte auf einem externen Datenträger gesichert werden. Denn wenn dieser Schlüssel verloren geht, sind die verschlüsselten Dateien unwiderruflich unlesbar geworden! - Diese Verschlüsselung durch EFS wird jedoch wertlos, wenn die Kontodaten (Kontoname und Kennwort) von Unbefugten ausspioniert oder per Hacking geknackt werden.



Sichere Dateien - auf jedem Datenträger

Manche Windows 7-Versionen verfügen über eine **Bitlock-Laufwerksverschlüsselung**. Mit dieser wird eine Sicherheitslücke geschlossen: Verschlüsselte Datenträger (auch für USB-Sticks verfügbar als **Bitlocker to Go**) werden erst nach Eingabe eines Passworts oder Verwendung einer Smartcard lesbar.



1.8. Lernkontrolle – Fragen mit einer oder mehreren richtigen Antworten

Frage 1

Worum handelt es sich bei „Daten“?

- (A) um die Mehrzahl von Datum
- (B) um den ersten Kontakt in einem privaten Bereich eines Chatrooms
- (C) um Informationen, die in digitaler Form in Dateien gespeichert sind
- (D) um Informationen, die im Prozessor des Computers analog verarbeitet werden
- (E) um Informationen, die auch in einem Datensatz abgelegt sein können

Frage 2

Ordnen Sie folgende Begriffe ihrer Bedeutung zu:

Cybercrime

Zugang zu einem PC über Sicherheitslücken

ethisches Hacking

Internetkriminalität

Skimming

Datenklau als Folge sozialer Manipulation

Hacking

Ausspähen von Bank- oder Kreditkarten

Social Engineering

Aufspüren von Sicherheitslücken

Frage 3

Ein Brand löscht Daten durch Zerstörung ...

- (A) ... der Firewall
- (B) ... der CPU
- (C) ... der Festplatte
- (D) ... des RAM-Arbeitsspeichers
- (E) ... des USB-Sticks

Frage 4

Wofür steht der Begriff **Pretexting**?

- (A) Für das Ausspionieren von E-Mail-Texten
- (B) Für das Vorschlagen von sicheren Kennwörtern
- (C) Für missbräuchliche Nutzung personenbezogener Daten
- (D) Für das Vorbereiten von ethischem Hacking

Frage 5

Was schützt Daten zuverlässig vor unberechtigtem Zugriff?

- (A) Das Verstecken von Dateien
- (B) Das Verschlüsseln von Dateien
- (C) Zugang zu einem Intranet nur mit Benutzernamen und Kennwort
- (D) Verstecken von Daten durch „Information Diving“

Frage 6

Womit verhindern Sie das mutwillige oder absichtliche Verändern einer Original-Datei, die dennoch von allen gelesen werden darf?

- (A) durch die Vergabe eines Kennworts zum Öffnen der Datei
- (B) durch die Vergabe eines Kennworts zum Lesen der Datei
- (C) durch die Vergabe eines Schreibschutzkennworts
- (D) durch die Vergabe eines Speicherschutzkennworts

1.9. Das Wichtigste in Kürze

- ➔ Cybercrime und höhere Gewalt stellen Bedrohungen für Ihre Dateien, Daten und Informationen dar.
- ➔ Personenbezogene und Firmen-Daten müssen geschützt werden.
- ➔ Es gibt rechtliche Grundlagen für den Datenschutz und die Datenhaltung.
- ➔ Über zwischenmenschliche Beeinflussung zum Zweck des „Datenklaus“ (Social Engineering) werden Daten gesammelt. Die Folgen können Identitätsdiebstahl und Identitätsmissbrauch sein.
- ➔ Mit aktivierten Makro-Sicherheitseinstellungen, Passwörtern und Verschlüsselung von Dateien schützen Sie Ihre wichtigen Daten – und sich selber.