



ECDL
IT-Security

mit Windows 7–10 und
Internet Explorer 10–11

FEICHTINGER | Helmut

Dipl. Trainer

Microsoft Certified
Professional



Vorwort/Lernziele	4	6.3 Virens Scanner installieren	52
Bevor Sie beginnen ...	6	6.4 Einstellungen für die Virensuche festlegen	53
1 Daten, Sicherheit und Copyright	7	6.5 Datenträger gezielt auf Viren überprüfen	54
1.1 Was sind Informationen und Daten?	7	6.6 Auf gefundene Viren reagieren	55
1.2 Grundforderungen an Sicherheit	7	6.7 PC vor Spyware und Botnetzen schützen	57
1.3 Grundforderungen an die Vertraulichkeit	8	7 Sicher im Internet arbeiten	59
1.4 Datenschutz	11	7.1 Sicherheitsoptionen im Internet Explorer	59
1.5 Urheberrecht, geistiges Eigentum und Copyright	11	7.2 Sicherheitsprotokolle und -zertifikate erkennen	60
2 Computerkriminalität	12	7.3 Echtheit einer Webseite überprüfen	62
2.1 Cybercrime und Cyberspying	12	7.4 Sicherheitszonen für Webseiten nutzen	62
2.2 Formen des Identitätsdiebstahls	14	7.5 Datenschutzeinstellungen für Cookies ändern	63
2.3 Aufklärung	16	7.6 Blockieren von Inhalten	65
2.4 Übung	17	7.7 Privatsphäre schützen mit den InPrivate-Funktionen	65
3 Verschlüsselung und Passwortschutz	18	7.8 Automatisches Speichern	66
3.1 Grundlegende Informationen zur Kryptografie	18	7.9 Übung	67
3.2 Symmetrische Verschlüsselung	19	8 Umgangsformen und Sicherheit im Internet	68
3.3 Asymmetrische Verschlüsselung	20	8.1 Kinderschutz im Internet	68
3.4 Public Key Infrastructure	21	8.2 Facebook sicher und richtig nutzen	69
3.5 Den PC schützen	22	8.3 Privatsphäre und Standort bei Facebook einrichten	70
3.6 Übung	27	8.4 Anwendungen und Inhalte einschränken	73
4 Struktur und Sicherheit im Netzwerk	29	9 Sicher kommunizieren und mobil arbeiten	76
4.1 Wichtige Netzwerkabkürzungen	29	9.1 E-Mails signieren und verschlüsseln	76
4.2 Gründe und Ziele einer Vernetzung	30	9.2 Kommunikation mit VoIP und Instant Messaging	80
4.3 Netzwerkadministration	32	9.3 Mobile Geräte	81
4.4 Zugriffsschutz	32	10 Datensicherheitsmanagement	82
4.5 Firewalls	34	10.1 Datensicherung – Backups	82
4.6 Schutz drahtloser Netzwerke	37	10.2 Datensicherung unter Windows 7 durchführen	86
4.7 WLAN nutzen	39	10.3 Sicherung unter Windows 7 wiederherstellen	87
4.8 Übung	41	10.4 Elemente unter Windows 8.1 und Windows 10 sichern und wiederherstellen	91
5 Schadsoftware	43	10.5 Den Computer unter Windows 8.1 und Windows 10 zurücksetzen	93
5.1 Grundlagen der Internetsicherheit	43	10.6 Sensible Daten endgültig löschen	94
5.2 Grundkonzepte von Viren	44	A So finden Sie die Inhalte zu den Lernzielen	95
5.3 Würmer	46	Stichwortverzeichnis	102
5.4 Adware und Spyware	47		
5.5 Die Kontrolle über den eigenen PC verlieren	48		
5.6 Pharming	48		
5.7 Übung	49		
6 Schutz vor Viren und Malware	51		
6.1 Antivirenprogramme verwenden	51		
6.2 Erste Schritte bei einer Vireninfektion	52		

Vorwort

Ziele

Die Kandidatinnen und Kandidaten sollen verstehen, wie wichtig die Sicherheit von Daten und Informationen ist und die Grundsätze zum Datenschutz, zur Datenspeicherung, zur Datenkontrolle und zum Schutz der Privatsphäre kennen.

Bedrohungen für die persönliche Sicherheit durch Identitätsdiebstahl sowie die mögliche Gefährdung von Daten durch Cloud-Computing kennen.

Passwörter und Verschlüsselung zur Sicherung von Dateien und Daten einsetzen können.

Die Bedrohung durch Malware verstehen und Computer, mobile Geräte und Netzwerke vor Malware schützen sowie auf Malware-Attacken richtig reagieren können.

Übliche Sicherheitsmerkmale von Netzwerken und Drahtlosverbindungen kennen und Personal Firewalls und Persönliche Hotspots verwenden können.

Computer und mobile Geräte vor unberechtigttem Zugriff schützen und Passwörter sicher handhaben und ändern können.

Geeignete Webbrowser-Einstellungen verwenden können und wissen, wie man die Vertrauenswürdigkeit einer Website feststellt und sicher im Internet surft.

Verstehen, dass Sicherheitsprobleme bei der Kommunikation per E-Mail, VoIP, Instant Messaging und in sozialen Netzwerken sowie durch die Nutzung mobiler Geräte auftreten können.

Daten auf lokalen Speicherorten und in der Cloud sichern und wiederherstellen können sowie Daten sicher löschen und Geräte entsorgen können.

Lernziel

1. Grundbegriffe zu Sicherheit

- 1.1. Wert von Informationen
- 1.2. Persönliche Sicherheit
- 1.3. Sicherheit für Dateien

2. Malware

- 2.1. Arten und Funktionsweisen
- 2.2. Schutz
- 2.3. Problemlösung und -behebung

3. Sicherheit im Netzwerk

- 3.1. Netzwerke und Verbindungen
- 3.2. Sicherheit im drahtlosen Netz

4. Zugriffskontrolle

- 4.1. Methoden
- 4.2. Passwort-Verwaltung

5. Sichere Web-Nutzung

- 5.1. Browser-Einstellungen
- 5.2. Sicheres Surfen

6. Kommunikation

- 6.1. E-Mail
- 6.2. Soziale Netzwerke
- 6.3. VoIP und Instant Messaging
- 6.4. Mobile Geräte

7. Sichere Datenverwaltung

- 7.1. Daten sichern und Backups erstellen
- 7.2. Daten sicher löschen und vernichten



Für einen optimalen Lernerfolg verfügen Sie über folgende Kompetenzen:

- ✓ Sie arbeiten sicher mit Maus und Tastatur.
- ✓ Sie beherrschen den Umgang mit Windows.

Um die Lerninhalte des Buches praktisch nachzuvollziehen, benötigen Sie:

- ✓ Windows 7, 8, 8.1 oder Windows 10



Haben Sie eine andere Bildschirmauflösung als 1280 x 1024 Pixel festgelegt, kann das Aussehen der Fenster von den Abbildungen im Buch abweichen.

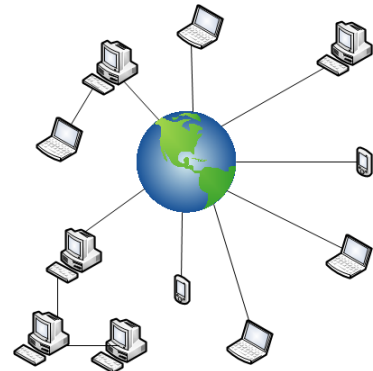
1

Daten, Sicherheit und Copyright

1.1 Was sind Informationen und Daten?

Unter Daten kann all das verstanden werden, was in digitaler Form bestehend aus Buchstaben, Zahlen oder Symbolen gespeichert werden kann. Zu Daten zählen erstellte Dokumente, Datenbanken oder Programmcode. Darauf aufbauend werden aus Daten infolge der Verarbeitung, Ausgabe oder Ausführung Informationen, die eine Bedeutung für den Benutzer/Empfänger haben.

Des Weiteren kann unter Informationen auch der Inhalt einer Nachricht oder Mitteilung verstanden werden, deren Hauptaufgabe die Vermittlung von Fakten ist. Informationen enthalten keine redundanten oder unnötigen Bestandteile.



1.2 Grundforderungen an Sicherheit

Unter dem Begriff „Sicherheit“ versteht man einen gefahrenfreien Zustand oder ein Zustand frei von unkalkulierbaren Risiken. Um klarer einzugrenzen, wie sich ein sicherer Zustand von einem unsicheren Zustand unterscheidet, gibt es einige Grundforderungen (oder Sicherheitsziele).

Sicherheit in der Informationstechnologie wird nicht ausschließlich durch den Schutz von Daten und Informationen gewährleistet. Eine weitere wichtige Rolle spielt dabei der physische Schutz von Computern und mobiler Geräte. So können beispielsweise Geräte beaufsichtigt, mit einer Zugangskontrolle versehen werden oder Geräte selbst und der Gerätestandort können gesperrt oder abgeschlossen werden.

Eine Diebstahlsicherung kann beispielsweise durch das Kensington-Schloss (Sicherheitskabel) sichergestellt werden. Geräte, die derart gesichert werden, sind mit einer entsprechenden Öffnung versehen, in die das Schloss eingeführt wird.

1.3 Grundforderungen an die Vertraulichkeit

Unter dem Sicherheitsziel der Vertraulichkeit (engl. confidentiality) wird verstanden, dass Informationen nur diejenigen erreichen, die diese Informationen auch besitzen dürfen.

Dies kann besonders beim Cloud-Computing problematisch werden, wenn die Anbieter, die meist im Ausland ihren Firmensitz haben, europäische Datenschutzrichtlinien (Datenkontrolle) nicht achten. Es kann aber auch vorkommen, dass in der Cloud gespeicherte Daten von Anbietern nach bestimmten Algorithmen durchsucht werden oder die Anbieter selbst gehackt werden und so private Daten öffentlich werden – der Verlust der Privatsphäre droht.



Bezogen auf die Kommunikation in Netzwerken ist das Sicherheitsziel der Vertraulichkeit vergleichbar mit dem Briefgeheimnis, bei dem nur der Sender und der Empfänger den Inhalt des Briefes kennen sollten, keineswegs aber der Postbote. Wenn Sie eine E-Mail an einen bestimmten Empfänger absenden, so erwarten Sie, dass auch nur der von Ihnen bestimmte Empfänger den Inhalt der E-Mail zu lesen bekommt.

Jede auf einem Computersystem gespeicherte Information dient einem bestimmten Zweck und in den meisten Fällen ist es nicht erforderlich oder nicht erwünscht, dass diese Informationen öffentlich zugänglich sind. Dies betrifft in Unternehmen neben den eigentlichen Mitarbeitern (einzelnen Personen) vor allem auch Dienstleister (beispielsweise Postboten oder Reinigungspersonal) oder externe Personen und Organisationen, denen bedingt durch die Mitarbeit im Unternehmen ein gewisses Vertrauen ausgesprochen wird. Da diese Gruppen zwangsläufig Zugang zu sensiblen Daten haben, besteht auch die Gefahr, dass Daten missbraucht werden.

In der realen Welt sind Schutzmaßnahmen für Vertraulichkeit z. B. ein Briefumschlag, in den man seine nicht öffentliche Nachricht steckt, oder eine abgesperrte Tür, die nur den Personen Zugang zu einem Raum gewährt, die den passenden Schlüssel besitzen.

Um Vertraulichkeit zu gewährleisten, können verschiedene Maßnahmen eingesetzt werden:

- ✓ Verschlüsselung von Dateien oder Nachrichten,
- ✓ Zugangskontrolle, die nur bestimmten Personen einen Einblick erlaubt,
- ✓ digitale Zertifikate.

Wie Integrität gewährleistet wird

Wenn mit Daten gearbeitet wird, muss ein sicheres System auch gewährleisten können, dass die Daten korrekt sind (engl. integrity). Es muss nach Möglichkeiten gesucht werden, Fehler bei der Übertragung von Daten zu verhindern oder wenigstens zu erkennen und diese gegebenenfalls zu korrigieren.

Ebenso wie der Schutz von Daten, Dokumenten und Systemen vor Manipulation (sowohl absichtliche als auch unabsichtliche bzw. aufgrund eines technischen Fehlers entstandene) spielt die Echtheit (**Authentizität**) der entsprechenden Daten eine große Rolle. Von Authentizität (engl. authenticity) wird dann gesprochen, wenn neben der Integrität auch gewährleistet werden soll, dass Informationen über den Urheber oder Verfasser der Daten übermittelt werden – sozusagen eine digitale Unterschrift.

Eine einfache E-Mail, die eine Bestellung enthält, wird vor Gericht mangels unverwechselbarer Unterschrift keinen Bestand haben: Der Inhalt könnte beispielsweise manipuliert sein, oder es wurde sogar der Absender der E-Mail gefälscht und der vermeintliche Auftraggeber weiß gar nichts von seiner Bestellung.

Durch die eigene Unterschrift auf einem Stück Papier belegen Sie, dass Sie mit dem Inhalt des Textes einverstanden sind und seine Konsequenzen akzeptieren. Da Ihre Unterschrift durch das Papier direkt (und relativ schwer trennbar) mit dem unterschriebenen Text zusammengebracht wird, ist hier die Verbindlichkeit gewährleistet. Aufgrund der Natur von Informationssystemen ist diese Untrennbarkeit von Inhalt und Unterschrift nicht ganz so einfach zu realisieren und zu garantieren.

Authentifizierung stellt in gewisser Weise eine detailliertere Sicht von Integrität als Sicherheitsziel dar, der durch die Einführung der digitalen Signatur (digitale Unterschrift) Rechnung getragen werden soll.

Als eine Forderung, die die Authentifikation erweitert und der digitalen Signatur erst einen Sinn gibt, lässt sich die **Verbindlichkeit** bzw. **Nichtabstreitbarkeit** (oder Non-Repudiation) einer digitalen Unterschrift definieren.

Ist in einem System die Verbindlichkeit für die Kommunikation sichergestellt, so kann ein Teilnehmer nicht zu einem späteren Zeitpunkt behaupten, die Kommunikation habe nicht oder mit einem anderen Inhalt stattgefunden.

Verfügbarkeit als Sicherheitsziel

Das dritte Hauptziel für die Sicherheit von Daten ist die Verfügbarkeit. Die Zusicherung der Verfügbarkeit gilt insbesondere für den Fall, dass Datenverlust durch Manipulation, Kriege oder höhere Gewalt (unabwendbare Ereignisse, wie Naturkatastrophen, Fluten oder Hochwasser und Stromausfälle) droht, und kann durch eine feuer-, wasser- und EMP(Elektromagnetischer Puls)-feste Auslegung der Serverräume und Datensicherung sichergestellt werden. Ein sicheres System muss gewährleisten können, dass Dienste und Daten zugreifbar und nutzbar sind.

Verfügbarkeit umfasst in der Regel logische Schutzmaßnahmen (zum Beispiel gegen versehentliches Löschen) genauso wie geeignete Maßnahmen, die einen Betrieb bei Störungen von Hard- und Software aufrechterhalten können. Hierzu zählen u. a. regelmäßige Datensicherungen, die die schnelle Wiederherstellung eines fehlerfreien Zustands ermöglichen.

Weitere Beispiele

- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Redundante Server-Systeme (doppelte Netzteile, Controller, RAID)
- ✓ Virtualisierung der Daten und deren Backup (NAS)
- ✓ „Watchdog“: Hard- oder Software, die das Funktionieren eines Systems überwacht
- ✓ Mehrfache Netzverbindungen
- ✓ Redundante Dienste
- ✓ Verteilte Anwendungen

Falsche Bedienung

Die Hauptursache für Sicherheitsprobleme liegt – im Gegensatz zu den vorsätzlichen Sicherheitsverletzungen – in der mangelnden Kompetenz der Mitarbeiter. Viele erhalten, wenn überhaupt, nur eine kurze Einarbeitung in die IT-Umgebung am Arbeitsplatz. Findet diese statt, so ist sie meist auf das Ziel „Erfüllung der Aufgabe“ ausgerichtet, nicht aber auf die Sicherheit im Betrieb.

So ist es nicht überraschend, wenn viele Sicherheitsprobleme durch Fehlbedienung seitens der Benutzer entstehen. Teilweise wird dies auch durch Software mit verwirrenden Dialogen und umständlichen Bedienkonzepten gefördert. Zu den wichtigsten Problemen gehören:

- ✓ versehentliches Löschen von Dateien,
- ✓ versehentliches Senden von sensiblen Daten an Unbefugte,
- ✓ falsche Änderungen an Datenbeständen.

Schaffung von Wissen über Vorschriften und Arbeitsvorgänge

Vielerorts wissen Mitarbeiter nicht um die speziellen Vorschriften, die für die IT-Sicherheit an ihrem Arbeitsplatz gelten. Noch so gründlich erarbeitete Sicherheitsrichtlinien können vom Mitarbeiter nicht berücksichtigt werden, wenn dieser niemals über deren Existenz unterrichtet worden ist. Besonders verheerend ist es, wenn z. B. der Posten eines Datenschutzbeauftragten oder IT-Sicherheitsbeauftragten intern einem beliebigen Mitarbeiter zugeteilt wird, der nicht über die notwendige Fachkompetenz zur Erfüllung dieser Aufgaben verfügt. Diese Person kann selbst beim besten Willen keine vernünftigen Sicherheitsrichtlinien (Policy) entwerfen.

Solange der einzige Mitarbeiter, dem die Policy bekannt ist, der IT-Sicherheitsverantwortliche ist, der sie erstellt hat, kann die Policy auch nicht wirksam sein. Deswegen ist eine Einführung in Vorschriften und Arbeitsvorgänge ein unerlässlicher Bestandteil der Einarbeitung.

Schulen Sie nicht nur das IT-Personal und die IT-Sicherheits-Mitarbeiter, sondern die gesamte Belegschaft. Die Wahrscheinlichkeit, dass ein erfahrener Administrator einen unverlangt von Unbekannten zugesendeten Mail-Anhang (Attachment) öffnet, ist deutlich geringer, als dass ein Mitarbeiter einer Nicht-IT-Abteilung aus Neugier ein derartiges Attachment ausführt.

Da ungeschultes Personal den Großteil der Mitarbeiter und somit die größte Angriffsfläche für Datenmissbrauch darstellt, sollten alle Mitarbeiter für Sicherheitsprobleme und ihre verschiedenen Erscheinungsformen sensibilisiert werden. Mitarbeiter sollten gleich zu Beginn des Arbeitsverhältnisses über Vorschriften mündlich bzw. schriftlich informiert werden. Darüber hinaus sollten Mitarbeiter gezielt nach Vorschriften fragen, so dass diese im Intranet veröffentlicht werden oder die Personalabteilung bzw. die EDV-Abteilung darüber informiert.

Richtlinien zur Datenaufbewahrung

Eine sichere Datenaufbewahrung und die Informationssicherheit sind in der ISO-Norm 27002 geregelt. Die Einhaltung dieser Richtlinie ist zwar nicht verpflichtend, sie ist aber international weit verbreitet und entspricht dem Hauptziel der Verfügbarkeit von Daten.

1.4 Datenschutz

Betroffene und Auftraggeber

Der Datenschutz in Österreich ist durch entsprechende Gesetze geregelt – den Datenschutzgesetzen. Bei der Erhebung und Verarbeitung von Daten unterscheidet das Datenschutzgesetz (DSG 2000) unter anderem zwischen Betroffenen und Auftraggeber. Unter Betroffenen wird gemäß DSG 2000 jede bestimmte bzw. bestimmbare natürliche Person verstanden, über deren Person Daten erhoben werden. Unter Auftraggeber versteht das DSG 2000 wiederum denjenigen, der personenbezogene Daten für sich selbst erhebt, verarbeitet und diese nutzt bzw. dies im Auftrag Dritter vornimmt. Die Interaktion, die Aufbewahrung und Kontrollmechanismen werden dabei durch das DSG 2000 (www.ris.bka.gv.at) geregelt.

Wichtige Regeln zum Datenschutz, zur Aufbewahrung und zur Kontrolle von Daten sind dabei die:

- ✓ **Transparenz:** Das informationelle Selbstbestimmungsrecht eines Betroffenen setzt die Kenntnis über die Struktur der Datenverarbeitung, die Prozesse, eingesetzten Techniken und Datenströme voraus. Nur mit diesem Wissen haben Betroffene die Möglichkeit, ihre Rechte wahrzunehmen.
- ✓ **Notwendigkeit (rechtmäßige Zweckverwendung):** Daten dürfen nur entsprechend dem DSG 2000 und dem Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, verwendet werden.
- ✓ **Verhältnismäßigkeit:** Das Verhältnismäßigkeitsprinzip sagt mit Bezug auf den Datenschutz aus, dass nur so viele Daten erhoben werden dürfen, wie zwingend für die Verarbeitung notwendig sind und das Maßnahmen von Staats wegen erforderlich, angemessen sowie geeignet sein müssen.

1.5 Urheberrecht, geistiges Eigentum und Copyright

Wer wird durch das Urheberrecht geschützt?

Das Urheberrechts bzw. Copyright bezieht sich ausschließlich auf die Person des Urhebers bzw. die Personen der Miturheber. Als Urheber wird der Schöpfer eines Werkes bezeichnet. Urheberrechte gelten für alle Werke, d. h. persönliche geistige Schöpfungen (Sammlungen von Werken, Daten oder anderen Elementen). Das Urheberrecht hat bis 70 Jahre nach dem Tod des Urhebers Gültigkeit.

Die Vervielfältigung, Verbreitung, Ausstellung sowie das Recht der öffentlichen Wiedergabe eines Werkes bedarf einer Genehmigung des Urhebers. Bei Verletzung des Urheberrechts kann der Urheber auf Schadensersatz etc. klagen.

- ✓ Software gilt im Sinne des Urheberrechtsgesetzes als Literatur.
- ✓ Alle Inhalte einer Internetseite (Texte, Bilder, Audio- und Videodateien) sowie deren Gestaltung sind durch das Urheberrechtsgesetz geschützt. Die enthaltenen Informationen können unter Nennung der Quelle in eigenen Texten genutzt werden.
- ✓ Informationen zum Urheberrecht in Österreich finden Sie im Internet unter [de.wikipedia.org/wiki/Urheberrecht_\(Österreich\)](http://de.wikipedia.org/wiki/Urheberrecht_(%C3%96sterreich)) oder www.ris.bka.gv.at

2

Computerkriminalität

2.1 Cybercrime und Cyberspying

Digitale Kriminalität

Cybercrime bzw. **Cyberspying** oder Computer-/Internetkriminalität bezeichnet u. a. den Diebstahl von Nachrichten, Informationen und Daten sowie die betrügerische Verwendung von Daten. Zu dieser illegalen und strafbaren Handlung zählt u. a. das Ausspähen im privaten Bereich (Verlust der Privatsphäre), das Abfangen von Wirtschaftsdaten als Teil der Wirtschaftskriminalität, die staatliche Überwachung und Spionage sowie die Nutzung und Verbreitung von illegaler Software und sogenannten Hacker-Tools.

Unter den Begriff „Cybercrime“ fallen:

- ✓ der Computerbetrug (der vorsätzliche Betrug mittels eines Computers),
- ✓ der Betrug mittels gestohlener Kreditkartendaten und PINs (Skimming),
- ✓ die Herstellung und Verbreitung von Schadsoftware (Malware),
- ✓ die Datenmanipulation und -sabotage,
- ✓ die Nutzung illegal erworbener Software oder ihre Verbreitung (Softwarepiraterie),
- ✓ das Ausspähen politischer Gegner und staatliche Überwachungs-/Spionageprogramme.

Einladung zum Diebstahl

Es muss aber nicht ausschließlich eine grob fahrlässige oder vorsätzliche Handlung eines Mitarbeiters vorliegen. Auch die Unwissenheit einzelner Benutzer kann dazu führen, dass Daten entwendet werden oder unbeabsichtigt verloren gehen. So besteht die Gefahr, dass Mitarbeiter unwissend schädliche Programme installieren. Durch die Verwendung von Trojanern (Programmen, die das Ausspionieren eines Computersystems ermöglichen), können Hacker auf empfindliche Daten zugreifen. Auch der Einbruch in ein Funkübertragungsnetz (Bluetooth oder WLAN) oder die Sabotage des eigentlichen Netzwerks sind Optionen, um Daten auszuspionieren.

Datenmitnahme

Mitarbeiter, die berechtigt sind, Informationen zu lesen, können diese Berechtigung auch nutzen, um eine Kopie dieser Daten anzufertigen. Spätestens dann, wenn die Notwendigkeit nicht mehr vorhanden ist, dass ein Benutzer auf bestimmte sensible Daten zugreifen kann, sollte ihm die entsprechende Berechtigung wieder entzogen werden.

Da nur schwer verhindert werden kann, dass während der befugten Arbeit mit sensiblen Daten bereits Kopien angefertigt werden, sollten in Bereichen mit hohem Sicherheitsanspruch Überlegungen angestellt werden, wie der Transport von Daten aus dem geschützten Bereich heraus verhindert werden kann.

Besonders die Verbreitung von USB-Anschlüssen an PCs und die hohe Verfügbarkeit von entsprechenden USB-Sticks stellen mangels ausreichender ins Betriebssystem integrierter Kontrollmethoden derzeit ein Problem dar. Zumal diese u. a. auch innerbetrieblich zur Datenübertragung genutzt werden und das dauerhafte Deaktivieren der entsprechenden USB-Schnittstellen am PC selbst nur schwer zu realisieren ist.

Folgende Aspekte sollten hier geprüft werden:

- ✓ Sind in den PCs USB-Ports oder Funkübertragungsschnittstellen (Bluetooth oder WLAN) installiert und aktiviert?
- ✓ Gibt es eine Möglichkeit für Benutzer, externe Laufwerke (USB-Sticks, DVD-Brenner, etc.) anzuschließen, um Daten zu kopieren?
- ✓ Besteht vom geschützten PC aus die Möglichkeit eines Internetzugangs?
- ✓ Wenn der Internetzugang nötig ist: Welche Programme sind zugelassen bzw. notwendig?

Erpressung/Manipulation

Verärgerte Mitarbeiter (zu wenig Gehalt, Kündigung o. Ä.) könnten erhebliche Schäden verursachen, indem sie z. B. die entwendeten Kundendaten oder Forschungsergebnisse veröffentlichen oder mit solchen Aktionen drohen. Mitarbeiter haben im Gegensatz zu Hackern viel leichter direkten Zugriff auf unternehmenskritische Daten und können Daten manipulieren, verkaufen, veröffentlichen oder löschen.

Hacken

Als **Hacken** wird das unberechtigte Eindringen in Computersysteme und Netzwerke verstanden, bei dem Sicherheitsvorkehrungen umgangen werden. Als Gegenstück zum Hacker, der meist einer Art Ehrenkodex folgt, gilt der **Cracker**, dessen Ziele meist krimineller Natur sind: Lücken in Netzwerken werden explizit gesucht, um diese zum Stehlen von Informationen, zur Verunglimpfung von Firmen bzw. Personen oder aus finanziellen Interessen ausnutzen zu können. Auch das Entfernen des Kopierschutzes von Spielen, Filmen und Musikalben wird als **Cracken** definiert.

2.2 Formen des Identitätsdiebstahls

Social Engineering – Informationen im sozialen Umfeld

Mitunter ist die einfachste Möglichkeit für einen Hacker nicht ein erfolgreicher Angriff auf die Firmen-Firewall oder das Knacken eines Passwortes. Vielerorts ist es erstaunlich einfach, die Konto- und Zugangsdaten von den Mitarbeitern des Unternehmens selbst in Erfahrung zu bringen.

Unter **Social Engineering** wird im Allgemeinen die soziale Manipulation von Menschen ohne Einsatz technischer Hilfsmittel verstanden. Dabei versucht der Hacker, unautorisierten Zugang zu Systemen oder Informationen zu bekommen, um Betrug, Industriespionage (nicht autorisierte Datenbeschaffung) oder Identitätsdiebstahl (Diebstahl und Verwendung von Benutzernamen und Passwörtern oder Bankdaten) zu begehen.

Pretexting

Durch Vorspielen eines erfundenen Szenarios (Vorspiegelung falscher Tatsachen) wird die Chance genutzt, dass ein beliebiges Opfer freiwillig personenbezogene Informationen preisgibt und vom Hacker gewünschte Aktionen durchführt. Oft werden im Vorfeld wesentliche persönliche Daten wie z. B. Geburtsdatum, Sozialversicherungsnummer, der letzte Rechnungsbetrag oder Bankauszüge des Opfers auskundschaftet. Mithilfe dieser Informationen wird die Legitimität des Abfragens von Daten vorgegaukelt.

Pretexting bedient sich mittlerweile häufig vermeintlich offizieller Dokumente, die angeblich von Polizei, Banken, Finanzämtern oder Versicherungen stammen. Formulare oder Webseiten sehen meistens dem Original zum Verwechseln ähnlich. Der sogenannte Pretexter muss einfach ein vorgefertigtes Protokoll mit Fragen versenden und sich auf potenzielle Rückfragen zukünftiger Opfer vorbereiten.

Social Engineering über das Telefon

Die häufigste Variante des Social Engineerings wird über das Telefon oder mobile Geräte durchgeführt. Der Hacker gibt sich gegenüber dem Angerufenen als Mitarbeiter des Helpdesks (Informationsdienstes) oder als ein Kollege aus, der zur Behebung eines dringenden Problems schnell ein Passwort benötigt.

Online Social Engineering

Im Gegensatz zum Social Engineering über das Telefon nutzt das Online Social Engineering das Internet (mithilfe mobiler Geräte) selbst, um neue Informationen zu gewinnen:

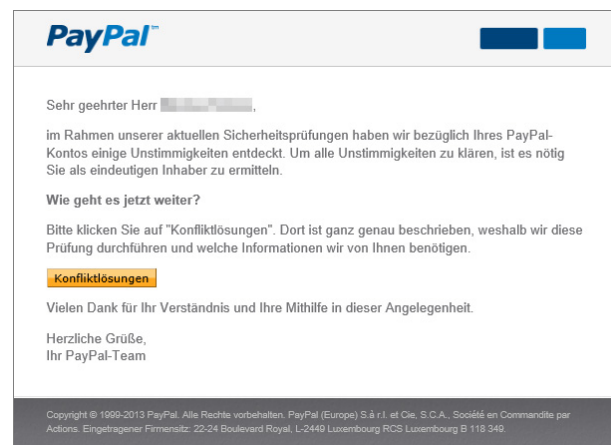
„Sie könnten gewinnen!“, heißt es möglicherweise in einer E-Mail an einen Mitarbeiter. Um an dem Gewinnspiel teilzunehmen, muss er nur schnell einen Fragebogen ausfüllen und ein paar Details zu seinem Arbeitsplatz erläutern o. Ä. Viele Menschen denken bei der Aussicht auf einen Gewinn nicht an den Wert der Informationen, die sie in ein Formular unbekannten Ursprungs eingeben.

Phishing

Eine weitere Variante der Social-Engineering-Angriffe ist das sogenannte Phishing (engl. Kunstwort aus „password“ und „fishing“: Passwortfischen). Bei dieser Art des Internetbetrugs werden zuerst massenhaft Mails verschickt, die vorgeben, z. B. von Online-Zahlungsdiensten wie PayPal oder von Auktionshäusern wie z. B. eBay zu sein. Diese betrügerischen und unerwünschten E-Mails gleichen meist in ihrem Erscheinungsbild den E-Mails der Originale. Es kann aber auch vorkommen, dass diese E-Mails viele Rechtschreibfehler (nicht verwendete Umlaute) und keine persönliche Ansprache enthalten.

Eine weitere beliebte Phishing-Methode ist das Versenden von Massenmails mit der Aufforderung, auf einen in der Mail enthaltenen Link zur eigenen Bank zu klicken. Der anzuklickende Link wurde mit diversen Techniken verschleiert und führt nicht auf die Original-Website, sondern auf eine Kopie. Als Vorwand dient oftmals eine Umstellung des Bankensystems bzw. Onlineauftritts, die angeblich die Eingabe der PIN (persönliche Identifikationsnummer) und mehrerer **TANs** aus einer Liste (Transaktionsnummer, die als **Einmal-Kennwort** z. B. beim Online-Banking nach einmaliger Verwendung ihre Gültigkeit verliert) erforderlich macht. Zu den Einmal-Kennwörtern zählen u. a. auch mobile TANs oder zur einmaligen Verwendung gestellte Kennwörter.

Der ahnungslose Nutzer, der auf diese Website gelangt und sich mit seinen authentischen Online-Zugangsdaten anmelden will, gibt so den Phishern seine Daten preis, die im Gegenzug dann sein Konto leerräumen oder die gestohlenen Zugangsdaten anderweitig ausnutzen.



Dumpster Diving bzw. Information Diving

Wörtlich übersetzt als „Mülleimertauchen“, ist Dumpster Diving ebenfalls eine mögliche Informationsquelle für Hacker. Gelingt es dem Hacker, Zugang zu weggeworfenen Akten, Memos, Organisationsplänen oder Ähnlichem zu bekommen, lässt sich aus diesen Unterlagen rekonstruieren, wer welche Rolle im Unternehmen spielt, wer welche Telefonnummer hat, zu welchen Zeiten er/sie im Büro anwesend ist etc.

Aus unsachgemäß gelöschten Datenträgern können Hacker vertrauliche Daten aus ausgemusterten Computern gewinnen. Oft wird in solchen Fällen der Datengewinnung, in Anlehnung an Dumpster Diving, von Information Diving gesprochen. Hierbei werden Informationen über installierte Software (z. B. Textverarbeitungsprogramme, Betriebssysteme, Computerspiele etc.) gewonnen. Ebenso können bei dieser Form der Informationsbeschaffung weitere Daten wie z. B. Kreditkarten-Informationen zugänglich gemacht werden.

Besonders schwerwiegend ist der resultierende Schaden für Unternehmen, wenn personenbezogene Kundendaten aus Unternehmen in den Bereichen Bildung, Versicherungen, Gesundheitswesen oder von Behörden „abgeschöpft“ werden.

Skimming

Beim Skimming (engl. für „Abschöpfen“) wird versucht, durch manipulierte Bankautomaten Informationen und Datensätze von Kunden abzufangen, um nachfolgend Konten zu „plündern“. Hierbei wird entweder mittels einer kleinen Funkkamera die Eingabe der PIN gefilmt oder das ganze Tastenfeld ausgetauscht, sodass die Eingabe der PIN über das manipulierte Tastenfeld zwischengespeichert werden kann. Von diesem Vorgang erfährt der Bankkunde nichts. Parallel dazu wird die in den Kartenslot eingeführte Bank- bzw. Kreditkarte durch ein zusätzlich am Karteneinzug angebrachtes Kartenlesegerät ausgelesen. Mit den so gewonnenen Daten lassen sich im Anschluss mithilfe von Magnetkartenrohlingen originalgetreue Kopien der ausgelesenen Bank- bzw. Kreditkarten herstellen.

Shoulder Surfing

Ähnlich wie beim Skimming werden beim Shoulder Surfing (auf Deutsch „Über die Schulter schauen“) Informationen und sensible Daten ausgespäht. Durch diese Art der Informationsgewinnung können die PINs von Bank- oder Kreditkarten oder Mail-Zugangsdaten an öffentlichen PCs in z. B. Internet-Cafés abgelesen werden. Selbst Eingaben am PC-Display können via Funkkamera, Fernglas und Teleskop aufgezeichnet werden.


Shoulder Surfing und Skimming kann vorgebeugt werden, indem bei jeglicher Eingabe personenbezogener oder wirtschaftlich relevanter Daten darauf geachtet wird, dass eine nachfolgende Manipulation oder das Abgreifen der Daten verhindert wird. Dies kann bei Eingabe der PIN durch einfaches Überprüfen des Geldautomaten und durch einen Blick über die eigene Schulter geschehen.

2.3 Aufklärung

Weitere Informationen zur Computerkriminalität und Formen des Identitätsdiebstahls finden Sie u. a. auf der Website des deutschen Bundesamts für Informationstechnik unter www.bsi-fuer-buerger.de. Wurden Sie selbst Opfer eines Identitätsdiebstahls, beispielsweise durch Phishing, oder wissen Sie etwas über eine missbräuchliche Nutzung sozialer Netzwerke, können Sie dies dem Service-Provider, den betreffenden Organisationen/Behörden, der Polizei oder den von Phishing betroffenen Unternehmen melden.

2.4 Übung

Computerkriminalität

Level		Zeit	ca. 10 min
Übungsinhalte	<ul style="list-style-type: none"> ✓ Verstehen, was Cybercrime ist ✓ Verstehen, was Identitätsdiebstahl ist ✓ Verschiedene Techniken des Identitätsdiebstahls kennenlernen 		
Übungsdatei	--		
Ergebnisdatei	Computerkriminalität.pdf		

1. Was wird unter dem Begriff „Cybercrime“ verstanden? Mehrere Antworten können richtig sein.

a	Die Datenmanipulation und -sabotage
b	Das anonyme Surfen im Internet
c	Das Spielen von PC-Spielen in der virtuellen Realität
d	Die Herstellung und Verbreitung von Schadsoftware (Malware)
e	Das Aufrufen von Webseiten
f	Der Datendiebstahl

2. Was ist Pretexting?

a	Das illegale Herunterladen von Texten
b	Das Durchsuchen von Festplatten nach illegalen Daten
c	Die illegale Datenbeschaffung durch Vortäuschen falscher Tatsachen

3. Was verbirgt sich hinter dem Begriff „Social Engineering“? Mehrere Antworten können richtig sein.

a	Vermeintliche Gewinnversprechungen, hinter denen sich ein Trojaner verbirgt
b	Die Unwissenheit anderer Menschen ausnutzen, um in ein Netzwerk einzudringen
c	Personen dahin gehend manipulieren, dass sie Bankdaten offenlegen
d	Die Nutzung sozialer Netzwerke

4. Worin unterscheiden sich Phishing und Skimming? Mehrere Antworten können richtig sein.

a	Beim Skimming werden Daten der Bank- bzw. Kreditkarte kopiert.
b	Phishing bezieht sich nur auf Bankgeschäfte, Skimming hingegen auf Online-Einkäufe.
c	Sie unterscheiden sich nicht.
d	Phishing nutzt die Unwissenheit von Menschen, um PINs und TANs auszuspionieren.

3

Verschlüsselung und Passwortschutz

3.1 Grundlegende Informationen zur Kryptografie

Was ist Kryptografie?

Ziel der Kryptografie (Verschlüsselung) ist es, Nachrichten oder Daten vor unberechtigttem Zugriff zu schützen. Dabei werden die Nachrichten bzw. Daten in eine Art Geheimschrift übersetzt und so zum vorgesehenen Empfänger geschickt. Die für die Nachricht gewählten Zeichen sollen so gewählt sein, dass nur der vorbestimmte Empfänger in der Lage sein sollte, den Inhalt der Nachricht wieder verständlich zu machen.

Der Begriff **Kryptografie** und die verwandten Disziplinen **Kryptologie** und **Kryptoanalyse** stammen aus dem Griechischen. „Kryptos“ bedeutet so viel wie „geheim“ oder „verborgen“. „Grafein“ steht für „schreiben“. Die Endung -analyse stammt von „analysein“, deutsch „entziffern“. „Logos“ steht für „Sinn“. Somit lassen sich also die drei Disziplinen wie folgt unterteilen:

- ✓ Kryptografie: die Wissenschaft der Geheimschrift
- ✓ Kryptoanalyse: die Kunst, Geheimschrift (unbefugt) entziffern zu können, den Code zu knacken
- ✓ Kryptologie: die Wissenschaft, die Kryptografie und Kryptoanalyse miteinander vereint

Informationen und Schlüssel

Das Grundproblem der Kryptografie ist, eine Nachricht zu verschlüsseln, sodass deren Inhalt während des Transports vor Unbefugten geschützt ist. Dies erfordert aber, dass der rechtmäßige Empfänger in der Lage sein muss, die Verschlüsselung wieder rückgängig zu machen.

Damit dies möglich ist, benötigt der Empfänger eine Zusatzinformation – einen Schlüssel. Ein ideales Verschlüsselungsverfahren ist so sicher, dass es nur mithilfe des passenden Schlüssels möglich ist, an den Inhalt der Nachricht zu kommen.

Um Nachrichten zu verschlüsseln, werden zwei unterschiedliche kryptografische Methoden angewandt:

- ✓ Symmetrische Verschlüsselung
- ✓ Asymmetrische Verschlüsselung

3.2 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung beruht auf dem **Prinzip des gemeinsamen geheimen Schlüssels**. Soll eine Nachricht ausgetauscht werden, wird diese mit dem geheimen Schlüssel verschlüsselt und mit dem gleichen Schlüssel wieder entschlüsselt. Voraussetzung für die symmetrische Verschlüsselung ist also, dass sowohl Sender als auch Empfänger einen gemeinsamen Schlüssel besitzen. Das Haupteinsatzgebiet der symmetrischen Verschlüsselung in der Informatik ist die Verschlüsselung von großen Datenmengen.

Nachteile von symmetrischen Verfahren

Schlüsseltausch

Obwohl symmetrische Methoden in der EDV inzwischen bewährt und weit verbreitet sind, haben sie alle einen gravierenden Nachteil: Sender und Empfänger müssen über den gemeinsamen geheimen Schlüssel verfügen, mithilfe dessen die Nachricht ver- bzw. entschlüsselt werden kann.

Ist Person A räumlich von Person B getrennt und besteht nun der Bedarf, eine Nachricht zum Schutz vor unbefugtem Mitlesen verschlüsselt zu übertragen, so stellt sich hier die Frage: Wie kann Person A den Schlüssel selbst sicher übertragen?

Ein Problem der symmetrischen Algorithmen ist, dass der Schlüssel selbst für seinen Transport einen sicheren Kanal benötigt. Wenn Sie also annehmen, dass Sie Verschlüsselung benutzen müssen, weil Sie wichtige Nachrichten über einen unsicheren Kanal schicken müssen, und befürchten, dass diese Nachrichten kompromittiert werden könnten, stellt sich die Frage, über welchen sicheren Kanal Sie den benötigten gemeinsamen Schlüssel übertragen können.

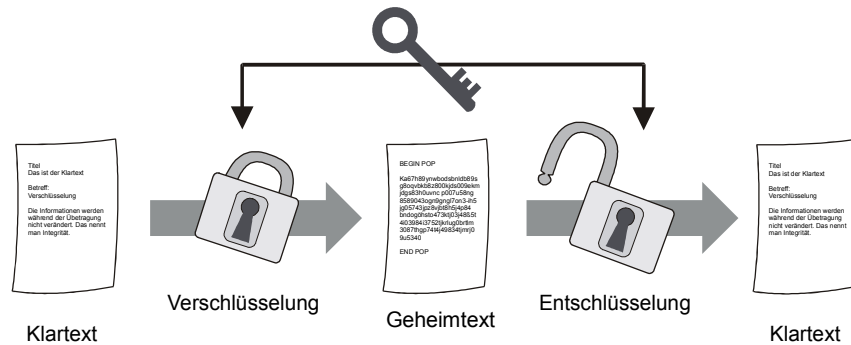
Schlüsselmanagement

Nehmen Sie an, Person A, Person B und Person C möchten in Zukunft sicher miteinander kommunizieren. Sie möchten, dass jeder mit jedem eine verschlüsselte Verbindung aufbauen kann. Die Schlüssel sollen aber jeweils nur zwischen zwei Partnern gültig sein.

Person A vereinbart also mit Person B einen Schlüssel 1 und mit Person C einen Schlüssel 2. Damit Person B kommunizieren kann, benutzt sie für Person A Schlüssel 1 und für Person C einen neuen Schlüssel 3. Person C wiederum benutzt für Person A den Schlüssel 2 und für eine Verbindung mit Person B den Schlüssel 3.

Jeder besitzt nun 2 Schlüssel und maximal 2 Personen kennen denselben Schlüssel:

- ✓ Person A 1, 2
- ✓ Person B 1, 3
- ✓ Person C 2, 3



Bei drei Personen existieren also 3 Schlüssel, jeder der Beteiligten muss sich 2 Schlüssel merken. Lassen Sie nun 10 Teilnehmer vereinbaren, ihre Kommunikation gegenseitig mit Schlüsseln zu sichern. Jeder der 10 Teilnehmer benötigt 9 Schlüssel für seine möglichen Partner. Das sind $10 \cdot 9$ Schlüssel. Da jeweils zwei Teilnehmer einen Schlüssel gemeinsam benutzen, ist die Anzahl der existierenden Schlüssel 45.

Die Anzahl der Schlüssel wächst quadratisch, da für n Teilnehmer $n*(n-1)/2$ Schlüssel benötigt werden. Spätestens hier wird klar, warum ein System mit vorher ausgehandelten symmetrischen Schlüsseln (**preshared keys**) nur bei kleinen Teilnehmerzahlen sinnvoll ist. Für das Internet mit seiner unüberschaubaren Anzahl an Teilnehmern wäre so etwas undurchführbar.

3.3 Asymmetrische Verschlüsselung

Was versteht man unter asymmetrischer Verschlüsselung (Public-Key-Verschlüsselung)?

Im Gegensatz zur symmetrischen Verschlüsselung existiert bei den asymmetrischen Verschlüsselungen für jeden Teilnehmer ein **Schlüsselpaar**. Dieses Schlüsselpaar setzt sich aus einem **geheimen Schlüssel (Private Key)** und einem **öffentlichen Schlüssel (Public Key)** zusammen.

Der geheime Schlüssel wird niemals weitergegeben und ist lediglich dem Besitzer bekannt. Der öffentliche Schlüssel dagegen kann gefahrlos verteilt werden. Öffentlicher und privater Schlüssel stehen zwar in einem bestimmten Verhältnis zueinander: Entscheidend dabei ist, dass es keine effiziente Möglichkeit geben darf, aus dem öffentlichen den privaten Schlüssel zu berechnen.

Beispiel: Will Person A an Person B eine Nachricht senden, muss Person A den öffentlichen Schlüssel von Person B besitzen. A verschlüsselt die Nachricht mit diesem öffentlichen Schlüssel. Nur Person B kann die Nachricht mit ihrem privaten Schlüssel wieder entschlüsseln. Damit ist gewährleistet, dass niemand anderes die Nachricht lesen kann.

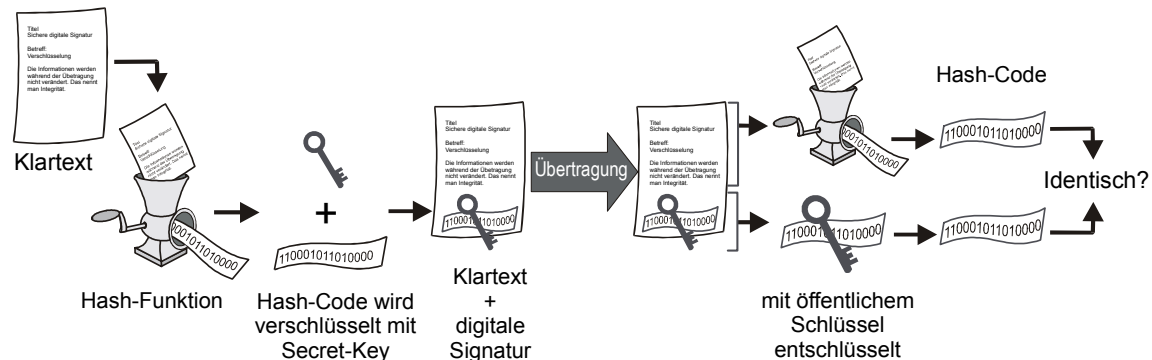
Der Einsatz von asymmetrischen Verschlüsselungsverfahren bietet neben der Verschlüsselung noch folgende weitere Möglichkeiten:

- ✓ Digitale Signatur
- ✓ Schutz vor Veränderung einer Nachricht
- ✓ Authentifizierung

Digitale Signatur

Durch eine digitale Signatur lässt sich die Identität des Nachrichtenabsenders eindeutig nachweisen. Digitale Signaturen sind in vielen Ländern (z. B. USA) bereits als rechtskräftige Unterschrift zugelassen.

Beispiel: Will Person A beweisen, dass die Nachricht von ihr stammt, signiert sie sie. Beim Empfänger wird mithilfe eines öffentlichen Schlüssels und der digitalen Signatur ein Wert berechnet, der Person A als Absender der Nachricht bestätigt.



Schutz vor Veränderung

Wird eine Nachricht digital signiert, wird automatisch eine Prüfsumme (Hashfunktion) des Dokuments berechnet. Die Hashfunktion ist so beschaffen, dass schon die nachträgliche Änderung von nur einem Bit zu einer anderen Prüfsumme führt. Dadurch kann der Empfänger zweifelsfrei feststellen, ob sich die Nachricht noch im ursprünglichen Zustand befindet.

Authentifizierung

Public-Key-Verschlüsselung kann sowohl zur Benutzer-Authentifizierung als auch zur Authentifizierung von Servern verwendet werden. Ein in der Praxis seit Langem eingesetztes Beispiel hierfür ist das Sicherheitsprotokoll SSL (Secure Sockets Layer), das es ermöglicht, einen sicheren Kommunikationskanal zu einer Webseite aufzubauen.

3.4 Public Key Infrastructure

Public-Key-Infrastrukturen

Eine Infrastruktur öffentlicher Schlüssel (PKI – Public-Key-Infrastruktur) ist eine Kombination von Software, Verschlüsselungstechnologien und Diensten, die den Umgang mit öffentlichen Schlüsseln ermöglicht. Um von einer PKI sprechen zu können, sollten folgende Funktionen zur Verfügung gestellt werden:

- ✓ Zertifizierungsstellen, die Zertifikate ausstellen und zurückziehen können
- ✓ Tools für die Schlüssel- und Zertifikatsverwaltung
- ✓ Anwendungen, die öffentliche Schlüssel verwenden können

Zertifikate sind eine Art „Verpackung“ für öffentliche Schlüssel und werden von Zertifizierungsstellen ausgestellt und unterzeichnet. Durch Zertifikate wird bestätigt, dass ein öffentlicher Schlüssel einem bestimmten Besitzer eindeutig zugeordnet ist. Die Zertifikate können verschiedene Attribute enthalten und für unterschiedliche Zwecke ausgestellt werden.

Die weitaus bekannteste Anwendung zur Public-Key-Verschlüsselung ist seit Langem das Verschlüsselungspaket PGP (Pretty Good Privacy). Sie können dieses Programm in verschiedenen Formen käuflich erwerben oder als Open-Source-Produkt kostenlos herunterladen und nutzen.

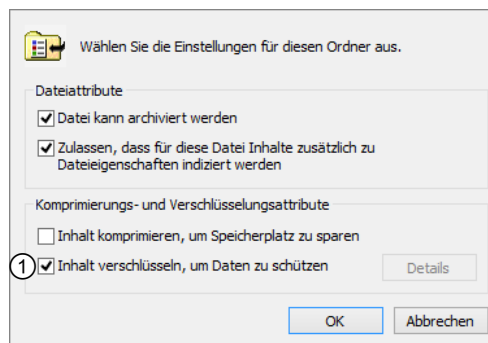
3.5 Den PC schützen

Dateien und Ordner verschlüsseln

Windows 7–Windows 10 verfügen über ein Dateisystem, das es Ihnen ermöglicht, Dateien zu verschlüsseln. Damit lässt sich ein unbefugter Zugriff auf die Daten verhindern.

Versucht ein unbefugter Benutzer, auf die verschlüsselten Daten zuzugreifen, wird eine Fehlermeldung angezeigt. Die verschlüsselten Dateien können nur von Ihnen wieder entschlüsselt werden. Sie können mit verschlüsselten Daten genauso arbeiten wie mit unverschlüsselten Daten. Die Daten werden automatisch und von Ihnen unbemerkt im Hintergrund entschlüsselt.

- ▶ Klicken Sie (z. B. im Explorer) mit der rechten Maustaste auf die gewünschte Datei oder den gewünschten Ordner und wählen Sie *Eigenschaften*.
- ▶ Betätigen Sie im Register *Allgemein* die Schaltfläche *Erweitert*.
- ▶ Aktivieren Sie ① und bestätigen Sie zweimal mit *OK*.
- ▶ Klicken Sie auf den Eintrag *Nur Datei verschlüsseln* bzw. *Änderungen nur für diesen Ordner übernehmen*.



oder Klicken Sie auf den Eintrag *Datei und übergeordneten Ordner verschlüsseln* bzw. *Änderungen für diesen Ordner, untergeordnete Ordner und Dateien übernehmen*.

- ▶ Bestätigen Sie abschließend mit *OK*.

Die betreffende Datei bzw. der betreffende Ordner und sein gesamter Inhalt (Unterordner und Dateien) werden nun verschlüsselt und können nur noch von Ihnen geöffnet werden. Der Vorgang kann bei größeren Ordnern eine gewisse Zeit in Anspruch nehmen.



Diese Methode der Verschlüsselung von Dateien und Ordnern schützt Ihre Daten nicht vor dem Zugriff staatlicher Institutionen. Möchten Sie Ihre Daten und Laufwerke vor dem Zugriff staatlicher Überwachungs- oder Spionageprogramme und Hackern/Crackern wirklich schützen, nutzen Sie zur Verschlüsselung Ihrer Daten und Laufwerke das Verschlüsselungspaket **PGP** (Pretty Good Privacy).

Wenn Sie im Fenster *Erweiterte Attribute* das Kontrollfeld ① deaktivieren und anschließend zweimal mit *OK* bestätigen, machen Sie die Verschlüsselung wieder rückgängig.

Die Namen verschlüsselter Dateien bzw. Ordner werden unter Windows 7 – Windows 10 grün angezeigt.

- ✓ Komprimierte Dateien oder Ordner lassen sich nicht verschlüsseln.
- ✓ Die Verschlüsselung von Daten auf einem Netzlaufwerk muss vom Administrator eingerichtet werden. Öffnen Sie solche Daten über das Netzwerk, werden die Daten unverschlüsselt übertragen.
- ✓ Wenn Sie eine unverschlüsselte Datei in einen verschlüsselten Ordner verschieben oder kopieren, wird diese automatisch verschlüsselt.

Die Notwendigkeit von Passwörtern

Viele Maßnahmen, die einen Computer sicherer machen können, werden oft aus Bequemlichkeit unterlassen. **Die Sicherheit eines Computers beginnt daher im Kopf des Anwenders.** Dazu gehört auch der Umgang mit Passwörtern. Sie dienen als Schutzmaßnahme, um bestimmte Daten vor unbefugten Zugriffen zu schützen. Sie stellen einen ersten und in den meisten Fällen auch ausreichenden Schutz dar. Ohne das notwendige Passwort kann kein Normalanwender die geschützte Datei oder den Datenbereich öffnen.

Sicherlich ist es für Insider und Inhaber von spezieller Software möglich, Passwörter zu „knacken“. Dennoch müssen auch diese Personen einen zum Teil nicht unerheblichen Aufwand an Zeit und Geduld aufwenden, um an einem Passwort „vorbeizukommen“. Selbst wenn der Angreifer alle Möglichkeiten kennt, wird er dennoch oft den Aufwand scheuen, sich mit dem Passwortschutz auseinanderzusetzen. Leichter ist es, sich einen ungeschützten Computer zu suchen.

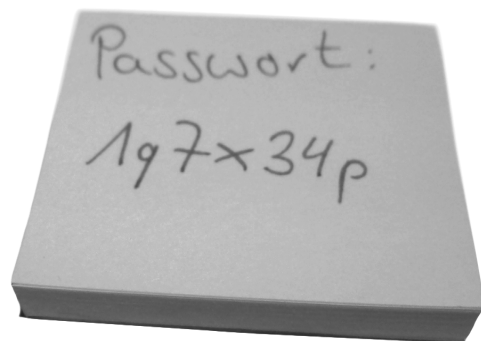
Achten Sie darauf, Passwörter, Schlüssel und Zertifikate nicht offen zu legen oder zu verlieren und verwenden Sie unterschiedliche Passwörter für unterschiedliche Dienste.

Falscher Umgang mit Passwörtern

Aber auch ohne Recovery-Tools gelangen Unbefugte oft leicht an Passwörter. Schuld daran ist der unbedachte Umgang der Benutzer mit Passwörtern. Viele Benutzer befürchten, dass sie das eigene Kennwort vergessen könnten, weshalb sie ein einfach zu merkendes Passwort wählen. Deshalb verwenden sie gerne kurze, einprägsame und vor allem reale Wörter, die möglichst noch einen Bezug zu persönlichen Vorlieben des Benutzers haben. So reicht es manchmal aus, etwas über diese Person in Erfahrung zu bringen. Hobbys, Bekannte, Familie etc. sind gute Wegweiser für die geheimen Codes.

Beim Umgang mit Passwörtern, Schlüsseln und Zertifikaten ist es nicht ungewöhnlich, dass diese an einer anderen Stelle hinterlegt werden. Beliebte Plätze zum Verstecken von Passwörtern sind beispielsweise die Rückseite der Tastatur, eine der oberen Schubladen im Schreibtisch, eine Haftnotiz am Monitor oder an der Pinnwand etc.

Eine häufige Möglichkeit mit Passwörtern zu arbeiten ist das ungeschützte Speichern sämtlicher Kennwörter auf dem Computer. Hacker kennen den Speicherort der Passwörter und werden dort sicherlich fündig.



Wenn Sie viele Zugangsdaten nutzen, können Sie diese mit einem professionellen Tool (sogenannten Passwort-Managern) verwalten. Ein Passwort-Manager ist ein Programm, dass alle Ihre Benutzernamen und Kennwörter/Geheimzahlen verschlüsselt in einer Datenbank speichert und diese nach Eingabe eines Passwortes abrufbar macht. Entsprechende Programme, wie z. B. *KeePas* gibt es für unterschiedliche Betriebssysteme und Plattformen. Der Nachteil des Passwort-Managers ist aber, dass der Anwender von seiner Passwort-Datenbank abhängig ist – und im Schadensfall (der Computer ist defekt) abhängig von regelmäßig erstellten Sicherheitskopien ist.

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung dient als Identitätsnachweis und kombiniert dabei unterschiedliche und voneinander unabhängige Komponenten. Dies kann am Beispiel einer Zwei-Faktor-Authentifizierung einerseits die alltägliche Komponente bestehend aus Benutzername und Passwort sein, andererseits eine weitere Komponente bestehend beispielsweise aus der Zusendung eines Einmalpasswortes via SMS.

Passwörter richtig erstellen

Vor allem mit der richtigen Auswahl des Passwortes können Sie dazu beitragen, dass das einfache Erraten der Zeichenfolge fast unmöglich wird. Je einfacher ein Passwort ist, desto leichter kann es auch herausgefunden werden.

- ✓ Erfinden Sie möglichst lange Passwörter (mindestens 12 Zeichen).
- ✓ Die Passwörter sollten aus einer Kombination von groß- und kleingeschriebenen Buchstaben, Zahlen und Sonderzeichen bestehen. (Verwenden Sie keine Zeichensatzspezifischen Sonderzeichen, sondern Zeichen wie ; , - _ (), weil manche Server andere Zeichensätze nutzen.)
- ✓ Das Passwort sollte kein bestehendes und verständliches Wort sein. Nehmen Sie beispielsweise einen Satz, den Sie sich merken können, und verwenden Sie nur die Anfangsbuchstaben der Wörter.
- ✓ Vermeiden Sie Passwörter, die mit Ihren Hobbys, der Familie etc. in Verbindung stehen.
- ✓ Ändern Sie je nach Wichtigkeit in regelmäßigen Abständen die Passwörter.
- ✓ Verwenden Sie nicht dasselbe Passwort für unterschiedliche Dienste.
- ✓ Speichern Sie keine Passwörter für den Zugang zum Internet, E-Mail- oder Firmennetz auf dem Computer.
- ✓ Wechseln Sie sofort das Passwort, wenn Ihr Passwort Dritten bekannt geworden ist.

Beispiel für ein sicheres Passwort

Eingabe	Merksatz
HM!Gwhu11UeDe?	Hallo Markus! Gehen wir heute um 11 Uhr einen Döner essen?

Im Internet können Sie auf der Website des Datenschutzbeauftragten des Kantons Zürich (www.passwortcheck.ch) und auf der Website des Anti-Viren-Software-Herstellers Kaspersky (www.blog.kaspersky.de/password-check) die Sicherheit von Passwörtern überprüfen.

Biometrische Zugangskontrolle

Neben der regulären Passworteingabe hat sich in den vergangenen Jahren eine weitere Form der Zugangskontrolle etabliert: die Zugangskontrolle basierend auf biometrischen Informationen, wie beispielsweise einem Fingerabdruck. Um eine biometrische Zugangskontrolle zu gewährleisten, werden im Vorfeld biologisch einzigartige Messdaten des Benutzers erfasst und ausgewertet. Werden Eigenschaften gefunden, von denen angenommen werden kann, dass sie für ein bestimmtes Individuum eindeutig sind, so kommen sie als Grundlage für ein Authentifizierungsverfahren in Betracht.

Folgende Merkmale werden häufig bei biometrischen Verfahren genutzt:

- ✓ Fingerabdruck
- ✓ Handgeometrie
- ✓ Irismuster (Regenbogenhaut als Teil des Auges)
- ✓ Stimmuster
- ✓ Tippverhalten eines Benutzers beim Schreiben auf einer Tastatur
- ✓ Unterschrift auf einem Grafiktablett
- ✓ Venenmuster in Hand oder Finger
- ✓ Gesichtsgeometrie

Diese Verfahren der Zugangskontrolle können ebenso wie die reguläre Passworteingabe nicht vollständig vor Missbrauch durch Aufzeichnung personengebundener Daten schützen. Es besteht weiterhin die Gefahr, dass durch Diebstahl, z. B. durch Kopieren eines Fingerabdrucks, der Zugang zu Daten und Informationen manipuliert wird.

Dateien in Anwendungsprogrammen mit Passwort schützen

In vielen Programmen können Sie Dateien mit einem Passwort schützen und so ein unbefugtes Öffnen dieser Dateien verhindern. Im Folgenden wird exemplarisch erläutert, wie Sie dies unter **Office 2010** bzw. **Office 2013** erreichen.

- ▶ Klicken Sie in der geöffneten Office-Datei im Register *Datei* auf *Speichern unter*.
Klicken Sie unter Office 2013 zusätzlich auf *Computer* und *Durchsuchen*.
- ▶ Klicken Sie im Fenster *Speichern unter* auf die Schaltfläche *Tools* und wählen Sie den Eintrag *Allgemeine Optionen*.
- ▶ Im geöffneten Fenster *Allgemeine Optionen* können Sie im Feld ① ein Passwort zum Öffnen festlegen.
oder Legen Sie im Feld ② ein Passwort zum Ändern fest.
- ▶ Klicken Sie auf *OK*.
- ▶ Tragen Sie das Passwort im eingeblendeten Fenster erneut ein und bestätigen Sie mit *OK*.

Die Kennwörter werden beim Speichern der Datei mitgesichert. Beim späteren Öffnen der Datei werden Sie zur Eingabe des Kennworts aufgefordert.

- Möchten Sie Ihre Office-Dateien auch vor dem Zugriff staatlicher Überwachungs- oder Spionageprogramme schützen, nutzen Sie zur Verschlüsselung Ihrer Dateien das Verschlüsselungspaket **PGP** (Pretty Good Privacy).


Komprimierte Dateien mit Passwort schützen

Viele Archivierungsprogramme bieten die Möglichkeit, zu komprimierende Dateien mit einem Passwort zu schützen. Dies ermöglicht eine Grundsicherung vor dem Zugriff Dritter auf Ihre Daten. Zur Veranschaulichung dient das kostenlose Archivierungsprogramm *7-Zip File Manager*, das unter www.7-zip.de heruntergeladen werden kann.

- ▶ Klicken Sie unter Windows 7 und Windows 10 auf die Windows-Startschaltfläche und geben Sie im Suchfeld den Begriff *7-Zip* ein.
oder Tragen Sie unter Windows 8.1 auf dem Startbildschirm den Begriff *7-Zip* ein.
- ▶ Klicken Sie anschließend auf *7-Zip File Manager*.
- ▶ Markieren Sie durch Ziehen mit der Maus die zu archivierenden Dateien.
- ▶ Klicken Sie auf *Hinzufügen*.
- ▶ Wählen Sie im Fenster durch Klicken auf die Schaltfläche ① den Speicherort aus.
- ▶ Tragen Sie im Feld ② ein beliebiges Passwort ein und wiederholen Sie dieses im Feld ③.
- ▶ Klicken Sie abschließend auf *OK*.

3.6 Übung

Verschlüsselung und Passwortschutz

Level		Zeit	ca. 15 min
Übungsinhalte	<ul style="list-style-type: none"> ✓ Symmetrische und asymmetrische Verschlüsselung unterscheiden können ✓ Verstehen, was eine digitale Signatur ist ✓ Die Public-Key-Infrastruktur kennenlernen ✓ Verstehen, wie Passwörter richtig erstellt und aufbewahrt werden 		
Übungsdatei	--		
Ergebnisdatei	<i>Verschlüsselung und Passwortschutz.pdf</i>		

1. Welche Aussagen treffen auf die symmetrische Verschlüsselung zu?

a	Wie bei der asymmetrische Verschlüsselung existiert ein Private Key und ein Public Key.
b	Die symmetrische Verschlüsselung beruht auf dem Prinzip, dass Sender und Empfänger über den gleichen geheimen Schlüssel verfügen.
c	Der Austausch des geheimen Schlüssels muss selbst über einen verschlüsselten Kanal getätigt werden.

2. Welche Aussagen treffen auf die asymmetrische Verschlüsselung zu?

a	Alle Teilnehmer teilen sich einen Schlüssel.
b	Ein Schlüsselpaar setzt sich aus einem Private Key und einem Public Key zusammen.
c	Der Private Key wird an alle Teilnehmer weitergereicht.
d	Der Public Key kann gefahrlos verteilt werden.
e	Es besteht keine Möglichkeit, aus dem Public Key den Private Key zu berechnen.

3. Was ist eine digitale Signatur?

a	Eine elektronische Unterschrift basierend auf der symmetrischen Verschlüsselung
b	Ein digitaler Fingerabdruck oder ein Irisscan
c	Eine elektronische Unterschrift basierend auf der asymmetrischen Verschlüsselung

4. Wie und wo sollten Sie Passwörter aufbewahren?

a	Es ist völlig ausreichend, Passwörter auf dem PC in einer Textdatei zu speichern.
b	Passwörter sollten an einem einfach zu findenden Ort abgelegt werden.
c	Falls Passwörter auf dem Computer gespeichert werden, sollten diese in einem Passwort-Tool sicher aufbewahrt werden.

5. Welche Aussagen sind zutreffend?

a	Es ist ausreichend, ein Passwort einmal zu erstellen.
b	Passwörter sollten aus mindestens 10 Zeichen bestehen.
c	Passwörter sollten einen zusammenhängenden Sinn ergeben.
d	Ein Passwort soll so gestaltet sein, dass es für verschiedene Dienste einsetzbar ist.
e	Ein sicheres Passwort besteht aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen.
f	Wenn unautorisierte Dritte Zugang zum Passwort hatten, muss dieses in der Regel nicht geändert werden.

4

Struktur und Sicherheit im Netzwerk

4.1 Wichtige Netzwerkkürzungen

Grundsätzlich ist ein Netzwerk, wie das Internet selbst, eine Gruppe miteinander verbundener Systeme, die in der Lage sind, untereinander zu kommunizieren. Sobald mindestens zwei Rechner per Kabel oder durch drahtlose Verbindungen (Wireless) miteinander verbunden sind und Daten austauschen, können Sie von einem Computernetzwerk sprechen.

LAN	Das Local Area Network ist gekennzeichnet durch eine begrenzte geografische Ausdehnung auf ein Firmengelände oder im privaten Haushalt. (Bei großen Firmen können Entfernungen bis ca. 10 km vorkommen.) Im Normalfall werden keine Leitungen öffentlicher Anbieter genutzt, sondern das Netz unterliegt vollkommen der Aufsicht der Firma.
MAN	Ein Metropolitan Area Network zeichnet sich durch die regionale Ausdehnung auf das Gebiet einer Stadt oder eines Ballungszentrums aus. Entfernungen bis circa 100 km sind möglich und ausreichend, um den Kommunikationsbedarf in dieser Fläche abzudecken. An manchen Stellen findet sich hierfür auch die Bezeichnung „Citynetz“.
WAN	<p>Ein Wide Area Network, auch Weitverkehrsnetz genannt, zeichnet sich durch eine unbegrenzte geografische Ausdehnung aus. In seiner klassischen Form ist ein WAN ein Verbindungsnetzwerk für räumlich getrennte Rechenanlagen. In Bezug auf die Übertragungswege der Daten werden dabei in der Regel Leitungen von externen Firmen angemietet. Unternehmen können ein WAN z. B. als Verbindung zwischen zwei oder mehr LANs nutzen.</p> <p>Ab und zu taucht auch noch der Begriff Global Area Network auf. Er beschreibt im Grunde nur die Ausdehnung eines WANs auf eine weltweite und damit globale Dimension.</p>
PowerLAN	Ein PowerLAN oder Powerline Communication (PLC) verzichtet auf eine klassische Verkabelung und nutzt als Übertragungsmedium das Stromnetz. Die Informationen werden hier trägermoduliert mittels Adapter über die normale Steckdose im Hausnetz übertragen. Das PowerLAN kommt vorzugsweise im privaten Bereich zum Einsatz.

WLAN	Ein Wireless Local Area Network (drahtloses lokales Netzwerk) ist eine Variante eines LANs und unterscheidet sich von diesem nur durch das verwendete Übertragungsmedium. Anstelle von Kabeln erfolgt der Einsatz von Funktechnologie. Gelegentlich wurden in diesem Zusammenhang auch die Begriffe WaveLAN und Wi-Fi verwendet.
VLAN	Bei einem Virtual Local Area Network wird das lokale Netzwerk in logisch voneinander getrennte Netzwerke unterteilt, wobei alle VLANs das gemeinsame physikalische Netz nutzen. Dadurch wird ein flexibles Design, z. B. für Arbeitsgruppen, unabhängig von ihrem geografischen Standort, gebildet.

4.2 Gründe und Ziele einer Vernetzung

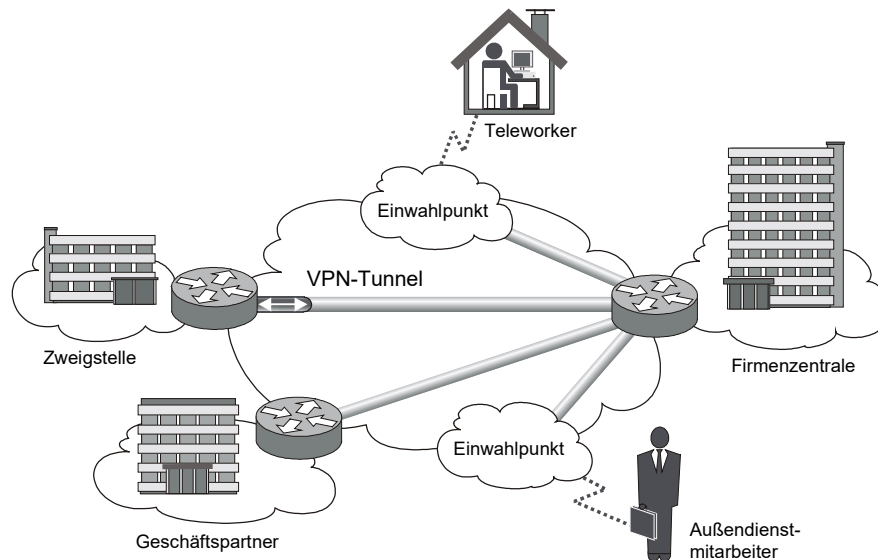
Was von Computer-Netzen erwartet wird

Ein Netzwerk bietet Vorteile gegenüber einer Einzelplatzumgebung. Allerdings ist der Einsatz auch mit einigem Aufwand verbunden. Umso mehr muss vor der Entscheidung für ein Netzwerk der zu erwartende Nutzen analysiert werden. Der Hauptgrund für die nicht unerheblichen Investitionen liegt letztendlich immer bei den zu erwartenden ökonomischen und unternehmerischen Vorteilen. Folgende Gründe sprechen für eine Vernetzung:

- ✓ Verbesserte Kommunikation
- ✓ Steigerung der Effektivität im Datenverbund
- ✓ Einfache und effiziente Datensicherung
- ✓ Kostensenkung im Funktionsverbund
- ✓ Absicherung der Verfügbarkeit
- ✓ Optimierung der Rechnerauslastung
- ✓ Optimierung der Wartung
- ✓ Zugriff auf einen gemeinsamen Datenbestand
- ✓ Gemeinsame Nutzung von Netzwerkressourcen, z. B. beim Drucken

Gründe für ein Virtual Private Network (VPN)

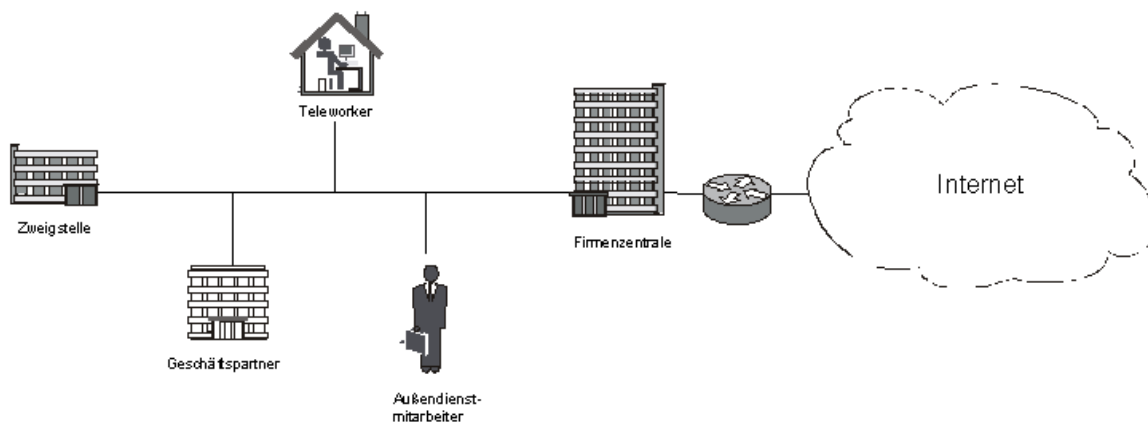
In Unternehmen, bei denen Zweigstellen oder Außendienstmitarbeiter Zugang zu Ressourcen der Firmenzentrale benötigen, wird meist mithilfe eines lokal genutzten Internetzugangs auf ein Virtual Private Network (VPN) zurückgegriffen. Ein Außendienstmitarbeiter könnte also über die Einwahl bei einem Internetprovider über das Internet Zugang zu Ressourcen in der Firmenzentrale bekommen, oder ein Teleworker, der beispielsweise im Home-Office arbeitet, könnte per Internet-Flatrate angebunden sein.



Da das Internet jedoch ein öffentliches Netz ist und so theoretisch jeder die übertragenen Daten an den Knotenpunkten abfangen oder sogar manipulieren könnte, müssen Möglichkeiten gefunden werden, wie dies verhindert werden kann. Hier bieten sich Methoden der Kryptografie als Lösung an.

Mit einer VPN-Verbindung können Datenpakete beispielsweise zwischen Außendienst-Rechner und Firmenzentrale verschlüsselt und signiert über das Internet übertragen werden.

Für den Anwender sieht es also so aus, als würde er sich im LAN der Firmenzentrale befinden.



VPN, logisches Netzwerk aus Sicht der Teilnehmer

Auch eine Kopplung von zwei LANs (z. B. Firmenzentrale und Zweigstelle) ist mit einem VPN realisierbar. In diesem Fall müssen Pakete je nach Bedarf von der einen auf die andere Seite geschickt werden. Als Transportmedium kommt hier wieder das Internet zum Einsatz.

Da in VPNs die Datenpakete, die ausgetauscht werden sollen, meist als Ganzes verschlüsselt und signiert innerhalb neuer Datenpakete verschickt werden, werden die Verbindungsstrecken zwischen zwei VPN-Übergabepunkten auch als VPN-Tunnel bezeichnet.

4.3 Netzwerkadministration

Der Aufgabenbereich von Netzwerkadministratoren in Firmennetzwerken erstreckt sich neben der Vernetzung einzelner PC-Arbeitsplätze über die Vergabe verschiedener Zugriffsberechtigungen und Freigabe der Netzlaufwerke bis hin zu sicherheitsrelevanten Einstellungen (z. B. Malwarehandhabung innerhalb eines Netzwerkes) und der Installation von sicherheitsrelevanten Patches (Nachbesserung bzw. Korrektur einer Sicherheitslücke) und Updates.

Authentifizierung und Autorisierung

Zur Anmeldung an einem Computer oder Netzwerk müssen Sie Ihren Benutzernamen und Ihr Kennwort eingeben. Dieser Vorgang wird **Authentifizierung** genannt. Er ermöglicht es, einen Netzwerkbenutzer (eindeutig, wenn **jeder** Benutzer über ein **eigenes** Konto verfügt) einer bestimmten Person zuzuordnen.

Nach erfolgreicher Authentifizierung wird in Form der **Autorisierung** überprüft, welche Zugriffsrechte ein Benutzer im Netzwerk hat bzw. ob dieser die Erlaubnis hat, Software selbstständig zu installieren.

Kontenvergabe und Benutzerverwaltung

Hier geht es primär um das „Who is who“ im Netzwerk oder, anders ausgedrückt, um die Frage: „Wer darf wo im Netzwerk was tun?“. Dabei bringt eine zentrale Verwaltung und Kontenvergabe u. a. folgende Vorteile mit sich:

- ✓ Ein Benutzer (Netzwerkkonto) kann sich nur mit gültigem Namen und Kennwort am Netzwerk anmelden (einloggen). Er erhält dann Zugriff auf die benötigten Daten oder Programme und soll aus Sicherheitsgründen das Netzwerkkonto sperren und sich bei Nichtverwendung abmelden – beim Abmelden werden alle Apps geschlossen. Im Gegensatz dazu wird beim Sperren nur der Zugriff für Dritte untersagt, die Apps bleiben weiterhin aktiv.
- ✓ Benutzer mit gleicher Aufgabenstellung können zu Gruppen zusammengefasst werden und erhalten über ihre Gruppenzugehörigkeit gemeinsame Rechte im Netzwerk.
- ✓ Ein oder mehrere Administratoren verwalten Benutzer und Gruppen zentral.

Insgesamt lässt sich so eine systematischere und damit auch übersichtlichere Struktur des Netzwerks aufbauen. Auch unter dem Aspekt der Sicherheit ist es vorzuziehen, dass Administratoren festlegen, auf welchem Weg auf die Ressourcen zugegriffen werden darf.

4.4 Zugriffsschutz

Voraussetzungen

Beim Thema Zugriffsschutz geht es darum, festzulegen, wer auf welche Art auf Daten zugreifen darf. Im Zusammenhang mit Datei-Zugriffen geht es hier um die Unterscheidung zwischen den Rechten:

- ✓ kein Zugriff
- ✓ Lesen
- ✓ Lesen und Ändern

Jedes Server-Betriebssystem hat Mechanismen eingebaut, die den Zugriff auf seine Daten regeln. Sie bauen normalerweise auf zwei Voraussetzungen auf:

- ✓ Das verwendete System muss die Vergabe von Zugriffsrechten unterstützen.
- ✓ Einzelne Benutzer müssen voneinander unterscheidbar sein.

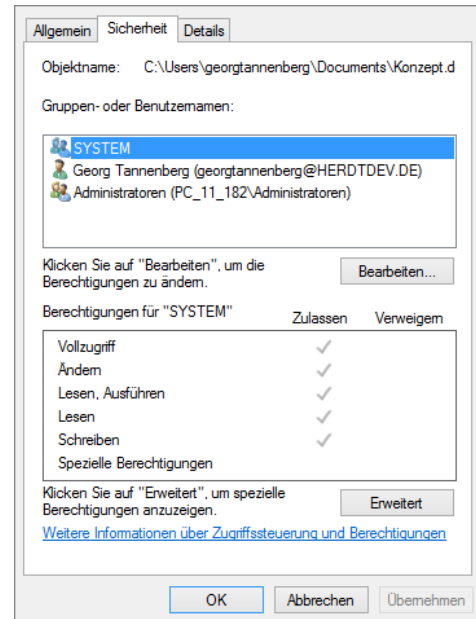
Dies wird über Benutzerkonten realisiert.

Mit den Benutzerkonten können Sie also festlegen, wer etwas darf, und mit den Zugriffsrechten bestimmen Sie, was der Benutzer darf. Das Zusammenbringen dieser beiden Informationen wird **Verreitung** genannt.

Dazu müssen Sie wissen, dass jedes Objekt, das Sie mit Rechten versehen können, diese Rechte in einer Zugriffsliste speichert. Im Weiteren geht es also darum, die entsprechenden Benutzerkonten in die jeweiligen Zugriffslisten einzutragen, und zwar mit den vorgesehenen Rechten.

Ein solches direktes Vorgehen wäre in großen Netzen mit vielen Benutzern sehr zeitaufwendig und fehleranfällig. Deshalb werden mehrere Benutzerkonten üblicherweise zu Gruppen zusammengefasst.

Wie das im Einzelnen genau funktioniert und was dabei alles möglich ist, unterscheidet sich teilweise sehr stark und ist abhängig vom eingesetzten Betriebssystem.



Dateirechte Lokale Zugriffsrechte

Überwachung

Ein anderer Aspekt des Zugriffsschutzes kann sein, zu wissen: Wer hat wann was womit gemacht? Systeme, die es ermöglichen, Rechte zu vergeben, sind normalerweise auch in der Lage, diese zu protokollieren.

Damit lässt sich dann auch protokollieren, wann Sie Ihren Rechner ein- und wieder ausgeschaltet haben. Dazu ein Hinweis: Protokolliert werden darf viel, aber sobald es um die Auswertung dieser Daten geht, hat der Betriebsrat oft Mitspracherecht.

In größeren Netzen gibt es oft einzelne Personen oder ganze Abteilungen, die überwiegend mit der Verreitung beschäftigt sind.

Ein wirksamer Zugriffsschutz setzt voraus, dass niemand Datensicherungen entwendet und zum Gelingen der guten Lösung jeder einzelne Benutzer verantwortungsvoll mit seinem Benutzerkonto (Benutzername und Passwort) umgeht.

4.5 Firewalls

Aufgaben einer Firewall

Der englische Begriff Firewall steht für eine Wand aus unbrennbarem Material, die in Gebäuden platziert wird, um die flächendeckende Ausbreitung von Bränden zu verhindern. Als Analogie in der Informationsverarbeitung soll eine Firewall, die sich klassischerweise an der Grenze zwischen dem eigenen Netzwerk und dem Internet befindet, die Ausbreitung von Gefahren aus dem Internet in das eigene Netz verhindern.

Eine Firewall ist ein System bzw. eine Gruppe von Systemen, deren Aufgabe darin besteht, die Kommunikation zu und von einem Netzwerk anhand von vorhandenen Regeln (Policies) zu kontrollieren. Beachten Sie, dass eine Firewall Regeln benutzt, um den Datenverkehr einzuschränken. Wurde eine Firewall eingerichtet, ohne dass sinnvolle Regeln erstellt wurden, ist sie relativ nutzlos.

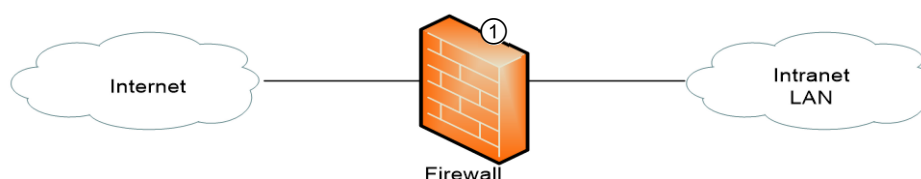


Obwohl Firewalls gewisse Schutzmaßnahmen gegen Hacker zur Verfügung stellen können, ist ihre Existenz alleine kein Allheilmittel. In vielen Firmen wird immer noch geglaubt, mit der Anschaffung einer Firewall wären alle Sicherheitsprobleme gelöst. Dieses falsche Sicherheitsgefühl kann schlimmere Folgen haben als das Bewusstsein, keinen Schutz zu besitzen.

Firewall-Konzepte

Je nach Schutzbedarf und Topologie (Anordnung bzw. Struktur) eines Netzwerkes können eine oder mehrere Firewalls sinnvoll sein. Wichtig in allen Fällen ist jedoch, dass sämtliche Kommunikationswege in das geschützte Netzwerk hinein und aus dem geschützten Netzwerk heraus über die Firewall laufen. Das beste Firewall-Konzept wird untergraben, wenn sich hinter der Firewall im internen Netz z. B. ein Einwahlserver oder ein WLAN-Access-Point befindet, der Zugriffe von außen erlaubt. Der WLAN-Access-Point dient als Schnittstelle (elektronischer Zugangspunkt) für kabellose Geräte, z. B. für einen Computer, der auf das Internet zugreifen will.

Die einfachste Lösung besteht aus einer Firewall ①, die am Übergabepunkt vom firmeneigenen Intranet (ein nicht öffentliches Firmennetzwerk) zum Internet den Datenverkehr überwacht.

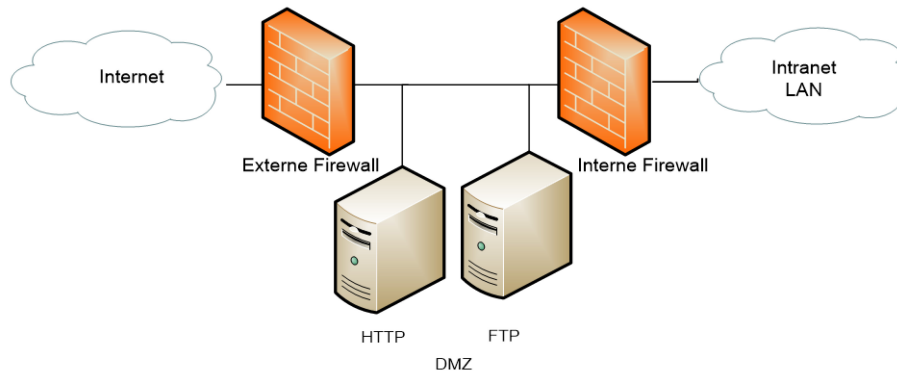


Obwohl diese Lösung relativ einfach zu realisieren ist, ist die damit erzielte Sicherheit vergleichsweise eher bescheiden. Sollte diese Firewall selbst einem Angriff zum Opfer fallen, so steht das Intranet dem Angreifer offen.

Darüber hinaus ist es problematisch, im Intranet einen Server zu betreiben, der vom Internet aus erreichbar sein soll. Wird eine Firewall so konfiguriert, dass Zugriffe von außen auf einen Server (z. B. auf einen WWW-Server) erlaubt sind, könnte dies wiederum auch ein Angriffspunkt für Hacker werden. Gelingt es einem Angreifer, Kontrolle über den WWW-Server zu erlangen, so kann dieser Zugriff auf andere Rechner im Netzwerk bekommen.

Als Antwort auf die Problematik, dass das Intranet geschützt werden sollte, bestimmte Rechner aber weiterhin von außen erreichbar sein sollen, werden die von außen zugreifbaren Server in einen vorgelagerten Bereich des Intranets verlagert. Die Rechner mit diesen speziellen Serveraufgaben befinden sich also im „Niemandland“ zwischen dem Intranet und dem Internet.

Als Fachausdruck für dieses Niemandland hat sich der Begriff „demilitarisierte Zone“ (DMZ) durchgesetzt.

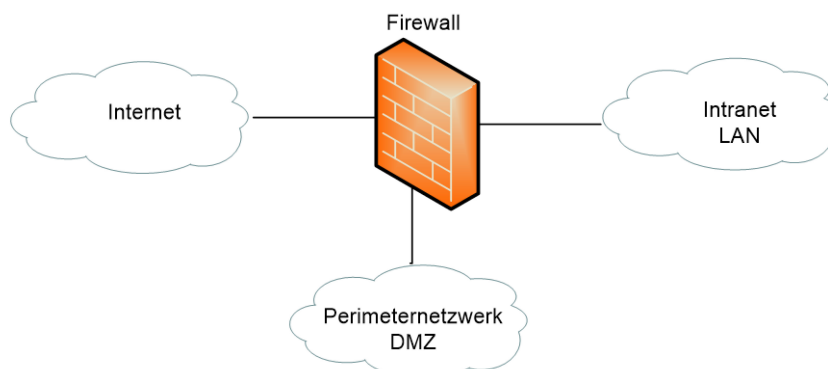


Im Normalfall wird die externe Firewall über Zugriffsregeln (erweiterte Zugriffs- bzw. Access-Listen oder Filter) so konfiguriert, dass sie den eingehenden Datenverkehr nur erlaubt, wenn das Ziel einer der in der DMZ installierten Serverdienste ist (in diesem Beispiel HTTP und FTP). Alle anderen Verbindungsversuche werden verworfen. Die interne Firewall sollte keinen Zugriff vom Internet in das Intranet erlauben, um die Systeme im Intranet zu schützen.

Umgekehrt kann die interne Firewall so konfiguriert werden, dass es Computern aus dem Intranet nur gestattet ist, entweder den firmeneigenen WWW-Server zu nutzen oder die E-Mail vom SMTP-Server abzuholen. Eine darüber hinausgehende Nutzung des Internets kann dann an der externen Firewall unterbunden werden, die außer den Servern in der DMZ keine Verbindungen erlaubt.

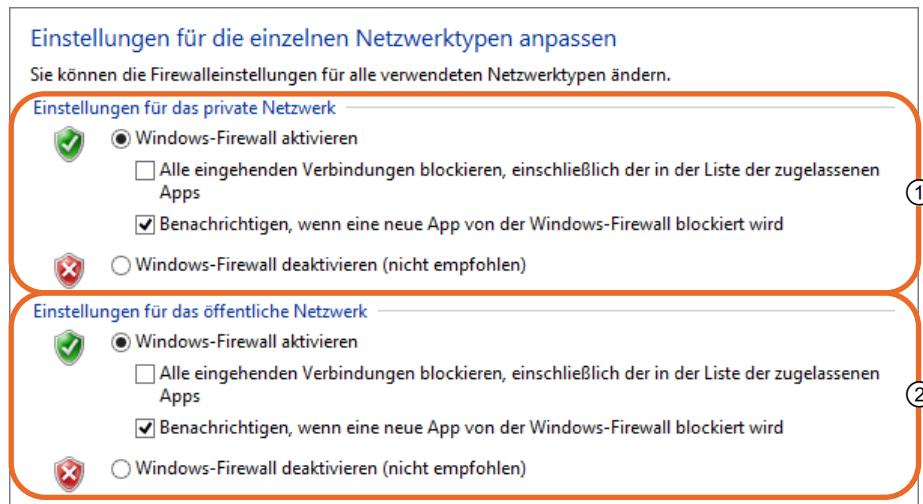
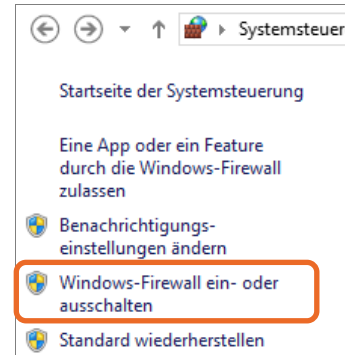
Würde in so einem Fall die externe Firewall oder einer der Server in der DMZ von einem Hacker übernommen, so blieben seine Zugriffsmöglichkeiten dank der internen Firewall nur auf die DMZ beschränkt.

Eine günstige Version einer demilitarisierten Zone, auch Perimeternetzwerk genannt, kann dadurch realisiert werden, dass an einem Firewallrechner bzw. einer Firewall-Appliance mehrere Schnittstellen vorhanden sind. So kann das Netzwerk ohne weiteren Hardwareaufwand, aber mit der Möglichkeit zur speziellen Konfiguration, eingebunden werden.



Windows-Firewall ein- bzw. ausschalten

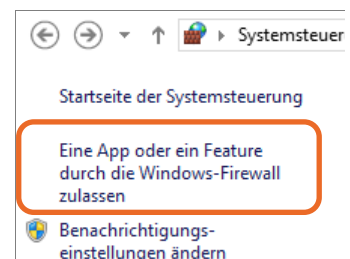
- ▶ Klicken Sie in der Systemsteuerung auf *Windows-Firewall*.
- ▶ Klicken Sie im linken Bereich auf *Windows-Firewall ein- oder ausschalten*.
- ▶ Klicken Sie im Bereich ① bzw. ② auf *Windows-Firewall aktivieren*, um die Firewall einzuschalten.
oder Klicken Sie auf *Windows-Firewall deaktivieren (nicht empfohlen)*, um die Firewall auszuschalten.



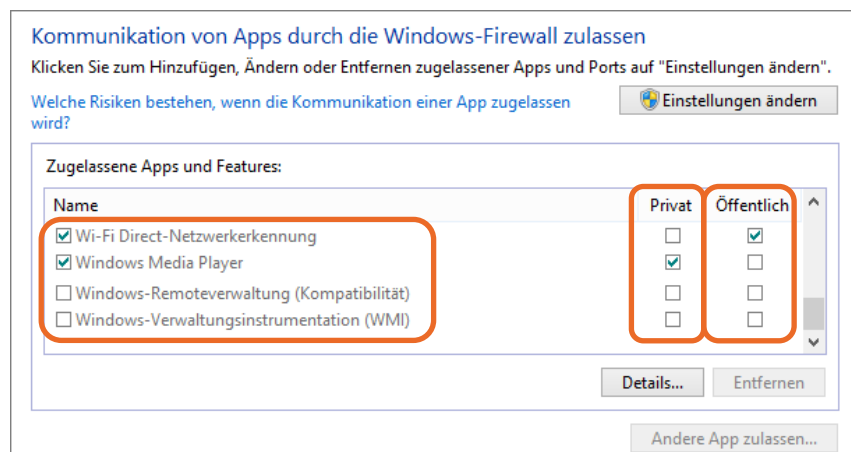
In der Windows-Firewall Apps zulassen bzw. blockieren

Um einzelne Apps (Programme oder Anwendung), Services oder Funktion zuzulassen bzw. zu blockieren, gehen Sie wie folgt vor:

- ▶ Klicken Sie in der Systemsteuerung auf *Windows-Firewall*.
- ▶ Klicken Sie im linken Bereich auf *Eine App oder ein Feature durch die Windows-Firewall zulassen*.
- ▶ Aktivieren Sie unter *Namen* das Kontrollfeld der App, die Sie in der Windows-Firewall zulassen möchten und aktivieren Sie unter *Öffentlich* bzw. *Privat* den Netzwerkbereich für den die Zulassung gültig sein soll.



Zum Blockieren einer App, klicken Sie unter *Namen* auf das entsprechende Kontrollfeld.



4.6 Schutz drahtloser Netzwerke

Standard-Installationen

In den überwiegend eingesetzten Access-Points (Zugangspunkt beispielsweise für WLAN) wird das Setup größtenteils durch Plug & Play erleichtert. So kann ein Systemadministrator ohne viel Aufwand neu zugekauftes WLAN-Equipment in sein vorhandenes Netzwerk einbinden. Dies kann jedoch ein Einfallstor für sogenanntes Wardriving (das Aufspüren von drahtlosen Netzwerken) sein, da oft Zugangsdaten und Kennwörter nicht oder nicht ausreichend geändert wurden. Vielfach werden die Werkseinstellungen für Benutzername und Passwort nicht geändert, teilweise ist auch kein sicheres oder gar kein Passwort konfiguriert. Gleiches gilt auch für herstellerseitig konfigurierte Service Set Identifier (SSID) des Access-Points.

So können von Wardrivern vielerorts ungeschützte WLANs gefunden werden, die für Lauschangriffe, Netzwerk-Übernahmen (Hijacking) oder man-in-the-middle-Angriffe ausgenutzt werden. Beim Hijacking wird beispielsweise eine Internetdomäne oder der Inhalt einer Webseite oder eines Internetaccounts (z. B. E-Mail) übernommen. Bei einem man-in-the-middle-Angriff befindet sich der Angreifer zwischen den Kommunikationspartnern und kann die Informationen einsehen und bei Bedarf manipulieren.

Zu empfehlen ist neben einem sicheren Verschlüsselungsprotokoll ein geeignetes Zugangspasswort, bestehend aus unzusammenhängenden Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Wenn die Hardware dies unterstützt, sollten Sie für die SSID Ihres Access-Points eine ähnliche Vorgehensweise wählen.

Um Wardrivern das einfache Auffinden von WLANs zu erschweren, schalten Sie die Übertragung der SSID ab, wenn dies in Ihrer Hardware möglich ist. Damit sich ein Client mit dem gewünschten WLAN über den Access-Point verbinden kann, muss dem Client die SSID des entsprechenden WLANs bekannt sein.

Um nun die SSID herauszufinden, können vorhandene Verbindungen abgehört werden. Das ist mit entsprechenden Tools auch kein Problem. Damit würden Sie allerdings, wenn es sich um ein geschütztes drahtloses Netzwerk handelt, gegen geltendes Recht verstoßen. Zudem kann das Abschalten der SSID das Beitreten neuer (erlaubter) WLAN-Geräte zum vorhandenen Netz etwas behindern. Insofern sollten Sie abwägen, ob das in Ihrem Unternehmen sinnvoll ist.

MAC-Filterung

Ebenso wie Standardnetzwerkkarten besitzen auch WLAN-Karten eine weltweit einmalig vorkommende MAC-Adresse (Media-Access-Control-Adresse). Einige Access-Points unterstützen eine MAC-Filterliste und lassen nur Verbindungen mit WLAN-Karten zu, deren MAC-Adresse für den Zugriff konfiguriert ist. Benutzen Sie dieses Feature, behalten Sie aber im Auge, dass auch MAC-Adressen von entsprechend ausgerüsteten Hackern gefälscht werden können. Zudem erfordert das händische Eintragen und Bearbeiten einer größeren Anzahl von MAC-Adressen einen zusätzlichen Zeitaufwand und ist nicht vergleichbar dem in einem kleinen Heimnetzwerk.

Die Verwendung eines sicheren Verschlüsselungsprotokolls, ein geeignetes Zugangspasswort, MAC-Filterung, die Abschaltung des SSID-Broadcasts und das Setzen einer Nicht-Default-SSID sollten zumindest den Gelegenheits-Surfer davon abhalten, zufällig Zugriff auf ein Netzwerk zu bekommen.

WEP – Wired Equivalent Privacy

WEP war das erste für WLANs verwendete Verschlüsselungsprotokoll. Wie der Name schon sagt, sollte es dafür sorgen, dass in WLANs eine Sicherheit erreicht wird, die der von konventionellen drahtgebundenen Netzen entspricht.



Von der Verwendung eines durch WEP geschützten WLANs ist abzuraten, da dieser Standard als unsicher gilt.

WPA – Wi-Fi Protected Access

Nachdem die gravierenden Probleme von WEP bekannt wurden, wurde fieberhaft an besseren Sicherheitsprotokollen gearbeitet. Dabei wurde allerdings auch klar, dass diese neuen Standards nicht in Kürze verfügbar sein würden.

Als Zwischenlösung wurde deswegen Ende 2002 der Standard WPA verabschiedet, der die wichtigsten Änderungen des endgültigen Sicherheitsstandards 802.11i vorwegnehmen sollte. Wi-Fi Protected Access führt eine neue Art der Verschlüsselung ein, die **TKIP** genannt wird.

Als eine der wichtigsten Verbesserungen in WPA ist die Tatsache anzusehen, dass das festgelegte Passwort in WPA nicht mehr der Verschlüsselungsschlüssel selbst ist, sondern die Schlüssel regelmäßig kryptografisch erneuert werden. Die Schlüssel werden automatisch in einem Zeitintervall erneuert, in dem es mit üblichen Methoden nicht mehr möglich erscheint, diese Schlüssel auch zu knacken. Sollte WPA zusammen mit einem Preshared Key (PSK) betrieben werden, besteht natürlich die Gefahr, dass man durch einen zu einfach zu erratenden PSK den Sicherheitsgewinn von WPA wieder zunichtemacht.

WPA2 – Wi-Fi Protected Access 2

2004 wurde der endgültige WLAN-Sicherheitsstandard mit der Bezeichnung IEEE 802.11i verabschiedet, der von einigen Herstellern als WPA2 bezeichnet wird. Die wesentlichen Kernpunkte, die im WPA schon vorweggenommen wurden (wie z. B. regelmäßige automatische Erneuerung der verwendeten Verschlüsselungsschlüssel) blieben erhalten. Gleichzeitig wird hier nun der moderne Standardalgorithmus AES (Advanced Encryption Standard) verbindlich vorgeschrieben.

Ein Funknetz, das mit 802.11i-Verschlüsselung betrieben wird, kann als wesentlich sicherer angesehen werden als ein WEP- oder sogar ein WPA-Netzwerk. Allerdings sollten Sie dabei beachten, dass bei Absicherung Ihres Netzes mit Preshared Keys Ihre Sicherheit davon abhängt, wie leicht oder schwer die verwendeten Preshared Keys (also die Passwörter) zu erraten sind.

4.7 WLAN nutzen

WLANs (persönliche Hotspots) richtig nutzen

Bei der Auflistung von drahtlosen Netzwerken in der Umgebung werden stets alle sichtbaren WLANs in Reichweite angezeigt. Bei der Nutzung von drahtlosen Netzwerken müssen Sie stets die Bestimmungen Ihres Unternehmens beachten. Dies setzt vor allem voraus, dass Sie sich nur in durch Ihr Unternehmen verifizierte Netzwerke einloggen.

Haben Sie die Berechtigung und den entsprechenden Schlüssel für ein geschütztes Netzwerk, ist eine sichere Nutzung gewährleistet. Das Login in ein offenes WLAN kann dahin gehend Schaden verursachen, dass einerseits nicht sichergestellt ist, dass Dritte nicht auf Ihre lokal gespeicherten Daten zugreifen oder aber Sie Ihr Firmennetzwerk gefährden. Andererseits greifen Sie möglicherweise ohne Befugnis unwissentlich in ein bestehendes Netzwerk ein.

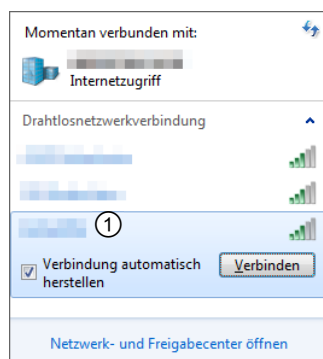
Persönlicher Hotspot

Ist kein WLAN in Reichweite, können Sie, mithilfe Ihres Smartphones oder Tablets einen persönlichen Hotspot einrichten und so mit dem Computer ins Internet gehen. Für den persönlichen Hotspot nutzen Sie dabei die mobile Datenverbindung Ihres Smartphones bzw. Tablets.

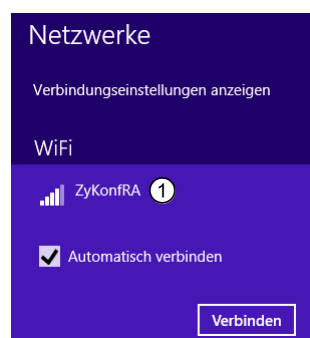
Sich mit einem WLAN unter Windows 7–10 verbinden

Möchten Sie sich unter Windows 7 mit einem ungeschützten bzw. geschützten WLAN verbinden, gehen Sie wie folgt vor:

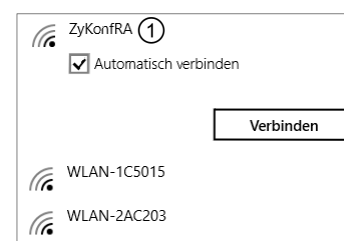
- ▶ Klicken Sie nach dem Aktivieren des WLANs im Infobereich der Taskleiste unter Windows 7 auf bzw. unter Windows 8–8.1 auf und unter Windows 10 auf .
- ▶ Klicken Sie auf den Namen ① eines offenen bzw. geschützten WLANs und klicken Sie *Verbindung automatisch herstellen* bzw. auf *Automatisch verbinden*.
- ▶ Klicken Sie auf *Verbinden*.



WLAN unter Windows 7



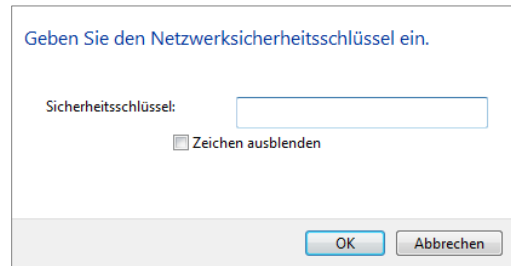
WLAN unter Windows 8–8.1



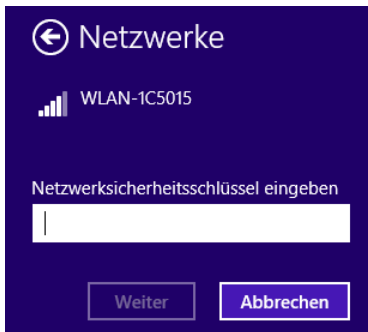
WLAN unter Windows 10

Handelt es sich um ein offenes WLAN, dessen IP automatisch vergeben wird, wird direkt eine Verbindung hergestellt.

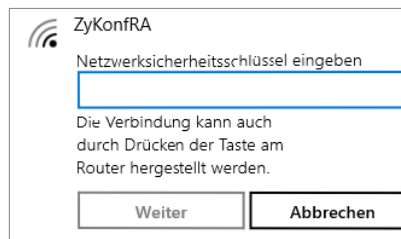
- ▶ Ist das WLAN geschützt, geben Sie unter Windows 7 im Feld *Sicherheitsschlüssel* das entsprechende Passwort ein.
oder Tragen Sie unter Windows 8–10 im Feld *Netzwerksicherheitsschlüssel eingeben* das entsprechende Passwort ein.
- ▶ Klicken Sie unter Windows 7 auf *OK*.
oder Klicken Sie unter Windows 8–10 auf *Weiter*.



WLAN unter Windows 7



WLAN unter Windows 8–8.1



WLAN unter Windows 10

Unter Windows die WLAN-Verbindung trennen

- ▶ Klicken Sie im Infobereich der Taskleiste auf unter Windows 7 auf unter Windows 8–8.1 auf und unter Windows 10 auf .
- ▶ Klicken Sie auf den Namen des verbundenen WLANs und wählen Sie *Trennen*.


Persönlichen Hotspot unter Android aktivieren und deaktivieren

- ▶ Tippen Sie unter *Einstellungen* auf *Mehr*.
- ▶ Tippen Sie auf *Tethering & mobiler Hotspot*.
- ▶ Tippen Sie unter *Tethering & mobiler Hotspot* auf *Mobiler WLAN-Hotspot* bzw. auf *WLAN-Hotspot*, um den persönlichen Hotspot zu aktivieren.

Zum Deaktivieren des persönlichen Hotspots tippen Sie unter *Tethering & mobiler Hotspot* erneut auf *Mobiler WLAN-Hotspot* bzw. auf *WLAN-Hotspot*.

4.8 Übung

Netzwerksicherheit

Level		Zeit	ca. 30 min
Übungsinhalte	<ul style="list-style-type: none"> ✓ Netzwerkadministration ✓ Zugriffsschutz ✓ Grundlagen der Internetsicherheit ✓ Schutz drahtloser Netzwerke 		
Übungsdatei	--		
Ergebnisdatei	<i>Sicherheit in Netzwerken.pdf</i>		

1. Welche der Aussagen sind zutreffend?

a	Unter Autorisierung wird das Überprüfen der Zugriffsrechte eines Benutzers im Netzwerk verstanden.
b	Authentifizierung und Autorisierung sind unterschiedliche Begriffe für die gleichen Vorgänge.
c	Bei der Kontenvergabe und Benutzerverwaltung geht es in erster Linie um das „Who is who“ im gesamten Netzwerk.

2. Was trifft auf den Zugriffsschutz zu?

a	Beim Thema Zugriffsschutz geht es darum, festzulegen, wer auf welche Art auf Daten zugreifen darf.
b	Bei einem wirksamen Zugriffsschutz bedarf es keiner Datensicherung.
c	Eine Protokollierung der Zugriffsrechte ist nicht möglich.

3. Welche Aussage ist zutreffend? Firewalls haben die Aufgabe ...

a	das Surfen der Benutzer im Web zu blockieren.
b	das System vor Angriffen zu schützen.
c	das firmeneigene Intranet zu blockieren.

4. Welche dieser Sicherheitsstandards und Verschlüsselungsprotokolle für drahtlose Netzwerke existieren?

a	WPA
b	SSID
c	TKIP
d	WIFI
e	MAC
f	WEP
g	WPA 2

5. Wie wird ein drahtloses Netzwerk richtig geschützt?

a	WLANs sind prinzipiell sicher.
b	<ul style="list-style-type: none"> ✓ Die SSID wurde versteckt. ✓ WPA wird als Verschlüsselung verwendet. ✓ MAC-Adressen-Filterung ✓ Der Access-Point wurde so positioniert, dass dieser nur geringfügig über die Gebäudegrenzen hinausstrahlt.
c	<ul style="list-style-type: none"> ✓ Die SSID wurde versteckt. ✓ WEP 2 wird als Verschlüsselung verwendet. ✓ Ein Mischbetrieb der Übertragungsstandards wurde unterbunden. ✓ MAC-Adressen-Filterung ✓ Der Access-Point wurde so positioniert, dass dieser nur geringfügig über die Gebäudegrenzen hinausstrahlt.
d	WEP wird als Verschlüsselung verwendet.
e	<ul style="list-style-type: none"> ✓ Die SSID wurde versteckt. ✓ WPA 2 wird als Verschlüsselung mit einem sicheren Passwort verwendet. ✓ Ein Mischbetrieb der Übertragungsstandards wurde unterbunden. ✓ Es findet eine MAC-Adressen-Filterung sowie eine Einschränkung der DHCP-Clients statt. ✓ Alternativ zur MAC-Adressen-Filterung wurde jedem Computer eine feste IP(Internet Protocol)-Adresse zugeteilt und diese im Access-Point eingetragen. ✓ Der Access-Point ist so positioniert, dass dieser nur geringfügig über die Gebäudegrenzen hinausstrahlt.

5

Schadsoftware

5.1 Grundlagen der Internetsicherheit

Gefahren aus dem Internet

Wird ein Rechner an das Internet angeschlossen, können Sie Dienste nutzen, die andere Rechner zur Verfügung stellen. Gegebenenfalls haben aber auch andere Benutzer des Internets oder staatliche Überwachungs- und Spionageprogramme die Möglichkeit, Dienste auf Ihrem Rechner anzusprechen oder sogar Daten aus Ihrem Firmennetzwerk zu nutzen bzw. zu entwenden. Das kann unter Umständen bedeuten, dass schädliche Programme, sogenannte Malware (aus dem Englischen *malicious* für böseartig und *software*), in Ihr System gelangt.

Gefahr	Beschreibung
Spyware (Spionage-Software)	Als Spyware (engl. spy = Spion) wird jede Software bezeichnet, die ohne das Wissen und das Einverständnis des Benutzers Daten an Dritte übermittelt. Häufig gelangt bei der Installation von Free-, Shareware oder Raubkopien Spyware heimlich auf das System des Benutzers. Meist dienen Spyware-Programme dazu, Informationen über das Surfverhalten des Nutzers an den Hersteller des Programms bzw. an Dritte zu übermitteln. Oft werden die Daten genutzt, um Werbebanner bzw. Popups bei Benutzern einzublenden, die speziell an deren Interessen angepasst sind.
Jugend-gefährdende Inhalte	Manche Webseiten stellen Inhalte dar, die unerwünscht bzw. für junge Internetbenutzer ungeeignet sind, z. B. Pornografie, rechts- bzw. links-extremistische Inhalte oder Gewaltdarstellungen.
Cyber-Mobbing	Cyber-Mobbing, Internet-Mobbing oder Cyber-Bullying bezeichnet das Verbreiten von Bosheiten bzw. falschen Behauptungen im Internet, um ein Opfer zu erniedrigen. Die Täter bleiben meist anonym und nutzen die Möglichkeiten des Internets (z. B. E-Mails, Chatrooms) für ihre Verleumdungskampagnen.
Betrug	Inhalte auf Webseiten können manipuliert sein, um von Ihnen eingegebene Daten „abzuhören“. Ein Beispiel hierfür sind sogenannte Phishing-Webseiten.

Gefahr	Beschreibung
Scareware	Durch die Verbreitung von Scareware wird versucht, Computerbenutzer zu verunsichern und einzuschüchtern. Diese sind meistens dazu bereit, für die Bereinigung von vermeintlich vorliegenden Gefahren für den Computer zu bezahlen.
Trojaner (trojanisches Pferd)	Programme, die dem Benutzer eine nützliche Funktion anbieten, aber bei Aufruf schädliche Funktionen im Hintergrund durchführen. Nach der Installation versuchen die meisten Trojaner, Benutzerdaten an bestimmte Adressen im Internet zu versenden. Trojaner installieren häufig auch zusätzliche Malware-Programme, beispielsweise ... sogenannte Backdoor-Programme, mit denen der betroffene Computer ferngesteuert genutzt werden kann, z. B. um massenhaft Spam-Mails (vom Empfänger nicht gewünschte E-Mails) zu versenden; sogenannte Keylogger, die Tastatureingaben (z. B. die Eingabe von Kennwörtern) mitverfolgen und über das Internet an einen Empfänger senden.
Rootkit	Ein Rootkit ersetzt wichtige Module des Betriebssystems des Rechners durch manipulierte Komponenten. Die Betriebssystem-Funktionen des Rootkits werden so verändert, dass der Rechner weiterhin seine gewohnte Arbeit ausführt. Allerdings werden sämtliche Prozesse und Aktivitäten, die auf den Hacker zurückzuführen sind, verborgen.
Keystroke Logging	Software- oder Hardware-Keylogger überwachen und protokollieren jede Eingabe (Tastaturanschlag) des Benutzers an einem Computer und übermitteln diese. Mit dieser Technik können Hacker auf persönliche Zugangsdaten zugreifen.
Ransomware	Unter Ransomware versteht man Schadprogramme, die Daten auf einem fremden Computer verschlüsseln bzw. den Zugriff auf selbige verhindern, um für die Entschlüsselung eine Art Lösegeld zu fordern.

Neben den oben erläuterten Malware-Varianten besteht bei Internetnutzern, die über eine Modem- bzw. ISDN-Verbindung auf das Internet zugreifen, eine Gefährdung durch **illegale Dialer** (Wählprogramme). Diese Programme richten ohne Wissen bzw. Zustimmung des Betroffenen eine neue DFÜ-Verbindung ein und wählen sich anschließend über teure Rufnummern ins Internet ein.

5.2 Grundkonzepte von Viren

Grundbauplan eines Virus

Grundsätzlich ist ein Virus ein Programm, das sich selbst vervielfältigt. Ein Virus verbreitet sich, indem er sich selbst in noch nicht infizierte Dateien kopiert. Der Schadcode wird ausgeführt, wenn diese Datei geöffnet wird oder ein bestimmtes Ereignis eintritt.

Ein Virus besteht aus mehreren funktionalen Komponenten, von denen eine obligatorisch ist, die anderen aber nicht unbedingt vorhanden sein müssen.

- ✓ Infektion
- ✓ Payload (Nutzlast)
- ✓ Tarnung

Der Teil des Computervirus, der sich mit der Weiterleitung beschäftigt, wird **Infektion** bzw. **Infektionsroutine** genannt. Im Laufe dieses Abschnitts werden Sie erfahren, welche Strategien zur Infektion Computerviren benutzen können.

Das Wort **Payload** bezeichnet die „Nutzlast“ eines Virus. Jedoch ist in seltensten Fällen von echtem Nutzen die Rede, sondern von den im Virus verankerten Schadensfunktionen. Je nach Absichten und Einfallsreichtum des Programmierers kann ein Virus die unterschiedlichsten Aktionen ausführen. Dies reicht von der Anzeige störender Bildschirmmeldungen über das Löschen einzelner Dateien bis hin zum Unbrauchbarmachen ganzer Datenträger.

Um nach der Infektion nicht entdeckt zu werden, enthalten die meisten Viren spezielle **Tarn-routinen**. Dies kann sich auf die Art und Weise der Infektion oder Manipulation des befallenen Systems auswirken. Die Tarnung kann so weit gehen, dass auf einem befallenen System die Entdeckung eines Virus selbst mit entsprechenden Scannern nicht mehr möglich ist.

Gefahr	Beschreibung
Bootsekturviren	<p>Um das Betriebssystem zu starten, wird durch das Einschalten des Computers auf den verfügbaren Datenträgern nach einem Bootsektor gesucht. Der Inhalt des Bootsektors wird in den Speicher geladen und ausgeführt. Der Code im Bootsektor enthält weitere Anweisungen, wie und wo die Startdateien des Betriebssystems zu laden sind.</p> <p>Bootsekturviren nutzen diese Vorgehensweise, um vor dem Start des eigentlichen Betriebssystems vom befallenen Rechner ausgeführt zu werden. Eine weitere Verbreitung dieser Viren erfolgt über die Infektion der Bootsektoren von CDs, DVDs oder USB-Sticks. Dadurch erhält der Virus die Chance, neue Rechner zu infizieren.</p>
Speicherresidente Viren	<p>Speicherresident ist ein Virus dann, wenn er nach seiner Ausführung im Speicher verbleibt und weiterhin aktiv ist.</p> <p>Ein speicherresidenter Bootsektorvirus würde bei seiner Ausführung zuerst über eine BIOS-Funktion (das Bios leitet den Start des Betriebssystems ein) den Wert für den maximal verfügbaren Speicher um den Betrag seiner eigenen Größe reduzieren. Anschließend kopiert sich der Virus in den als „nicht existent“ markierten Arbeitsspeicher.</p>
Dateiviren und Linkviren	<p>Ihre Aufgabe ist das Einschleusen eines Schadcodes in ausführbare Dateien und Bibliotheken des Betriebssystems.</p> <p>Bei Datei- und Linkviren sind folgende Infektionsmethoden gebräuchlich:</p> <ul style="list-style-type: none"> ✓ Overwrite-Infektion Der Virus überschreibt in einem solchen Fall die Originaldatei komplett und übernimmt dabei ihren ursprünglichen Namen. ✓ Infektion durch zusätzlichen Dateianhang Bei der häufigsten Infektionsmethode der Dateiviren versucht der Virus, sich am Ende der Wirtsdatei anzuhängen.

Gefahr	Beschreibung
Makro- und Skriptviren	<p>Makros werden zusammen mit der entsprechenden Dokumentdatei gespeichert. Sie sollten Funktionen enthalten, die dem Benutzer der Anwendungssoftware die Arbeit mit dem Dokument erleichtern.</p> <p>Innerhalb der Makrosprache werden zusätzlich zahlreiche Funktionen angeboten, die komplexe Operationen wie Dateimanipulationen oder sogar das automatische Versenden von E-Mails stark vereinfachen.</p> <p>Werden Makro-Sicherheitseinstellungen deaktiviert, kann ein Makrovirus beim Öffnen beispielsweise eines infizierten Word-Dokumentes ohne Wissen des Benutzers sofort aktiv werden. Die Infektionsroutine sucht nach weiteren Dokumenten, fügt den Virus als neues Autostart-Makro ein und versendet die Datei an alle im Adressbuch stehenden Empfänger. So ergibt sich hier ein extrem hohes Verbreitungs- und Schadenspotenzial.</p> <p>Daher wird empfohlen, die Makro-Sicherheitseinstellungen zu aktivieren bzw. aktiviert zu lassen und nur Makros aus sicheren Quellen auszuführen.</p>

Auch Flash-, Java- und Java-Script-Anwendungen können Schadcode enthalten. Durch entsprechend manipulierte Internetseiten wird versucht, sich über den Browser Zugriff auf die Festplatte zu verschaffen, um z. B. einen Virus zu installieren. Des Weiteren können auch Dateianhänge mit Makros sowie ausführbare Dateien, beispielsweise Dateien mit der Endung .exe oder .com, den Computer mit Malware infizieren.

5.3 Würmer

Im Gegensatz zu Viren, die zur ihrer Verbreitung eine Interaktion des Benutzers benötigen (z. B. Starten eines Programms), führen Würmer ein „Eigenleben“ in Rechnernetzen und vermehren sich selbstständig.

Die hybride Bedrohung

Seit dem Jahr 2008 spielen bekannte Würmer wie „mIRC“, „W32.Blaster“ oder „Sobig“ nicht mehr die wichtigste Rolle bei Computerinfektionen.

Ähnlich wie Hacker nutzen diese Würmer Exploits (Schadprogramme, die Sicherheitslücken des Anwendungsprogramms oder Betriebssystems ausnutzen) zur Ausführung des Schadcodes. Der Wurm sucht also vom Zielcomputer aus nach neuen Opfern. Durch den Zugriff auf Adressbücher in E-Mail-Clients und den automatischen Versand des Wurms an die so gewonnenen Adressen erschließt sich der Wurm mit jedem neu befallenen PC weitere Opfer.

Besonders gefährlich sind hybride Würmer, die sich in ihrer Ausbreitung nicht nur auf eine Sicherheitslücke und einen Verbreitungsweg spezialisieren, sondern eine ganze Reihe von Lücken in Server- und Clientsoftware kennen und diese systematisch durchprobieren.

„E-Mail-Würmer“ verschicken sich einfach als E-Mail an potenzielle Opfer und animieren den Empfänger meist durch geschickte Wahl des Dateinamens oder des Mailinhalts dazu, den E-Mail-Anhang zu starten. Dies ist auch eine Form des Social Engineerings.

5.4 Adware und Spyware

Den Computer ausspionieren

Der Begriff **Spyware** entstand, als Werbefirmen begonnen haben, spezielle Software zur Auswertung von Benutzerverhalten zu programmieren. Einmal installiert, erlauben diese Programme quasi die Rundum-Überwachung des betroffenen Computers. Dies geschieht ohne etwaiges Zutun des Benutzers. Je nach Fantasie des Programmautors ist derartige Software in der Lage, jegliche Benutzereingaben und Aktionen auszuwerten und an den Server des Werbetreibenden zurückzusenden.

Auffällig ist, dass Betreiber alles Mögliche unternehmen, um Dritten per Gerichtsbeschluss die Bezeichnung der eigenen Software als Spyware zu verbieten. Der eigentliche Zweck derartiger Software (Adware) wird in blumig formulierten, seitenlangen Lizenztexten, die meist niemand genau liest, versteckt. Eigentlich steht der Begriff **Adware** ausschließlich für Software, die kostenlos ist und sich über Werbeeinblendungen finanziert (Advertising software). Der Benutzer erklärt sich bei Benutzung der Software damit einverstanden, dass Daten über ihn gesammelt werden und entsprechende Werbung eingeblendet wird.

Kostenlose Downloads mit Tücken

Da sich Benutzer in den seltensten Fällen freiwillig Schadprogramme auf ihren Computern installieren, wird mit Tricks gearbeitet, um die Software verteilen zu können. Die offensichtlichste Methode ist, dem Benutzer die Software einfach beim Besuch einer präparierten Website automatisch „unterzuschieben“. Auch kann es vorkommen, dass dem Benutzer vorgegaukelt wird, ein „Update“ zu laden. Durchaus häufiger anzutreffen sind Versuche, die Software als Utility anzupreisen, das einen Nutzeffekt für den Benutzer hat.

Software-Bundles

Ebenfalls üblich ist es, Spywareprogramme an Softwareautoren zu vermitteln. Der Autor erhält für das Einbinden des Spywaremoduls in sein Programm Geld vom Spyware-Ersteller. Gegenüber dem Benutzer wird begründet, dass nur so die entsprechende Software als „Freeware“ zur Verfügung gestellt werden könne, weil sie anderweitig nicht finanzierbar wäre. Dieses Verfahren ist auch als „Sponsoring“ bekannt.

Häufig wird Spyware mit angeblicher Freeware gebündelt. Sie sollten bei der Installation von kostenloser Software aus dem Internet die Lizenzbedingungen aufmerksam lesen – auch wenn es keine Garantie gibt, dass der Hersteller die Verwendung von Werbesoftware in den Lizenzbestimmungen erwähnt.

5.5 Die Kontrolle über den eigenen PC verlieren

Entführte Browser

Besonders lästig kann es sein, wenn der Internetbrowser durch ein sogenanntes Browser Hijacking entführt wird und der Benutzer selbstständig keine Änderungen an den Einstellungen vornehmen kann. Es besteht aber auch die Möglichkeit, dass nach der Korrektur der jeweiligen Einstellungen (z. B. Startseite oder Lesezeichen) die unerwünschten Varianten spätestens nach einem Neustart des Systems wieder vorhanden sind. Hier wird parallel noch weitere Software im System verankert, die ständig überprüft, ob die vom Hijacker gewünschten Einträge noch vorhanden sind, und diese gegebenenfalls wieder erstellt.

Problemen durch Spyware können Sie am besten dadurch begegnen, dass Sie zum einen sehr genau darauf achten, welche Software Sie aus welchen Quellen installieren. Zum anderen sollten Sie spezielle Anti-Spyware benutzen, die im Stile von Virensclannern die Festplatte nach unerwünschten Programmen und Cookies durchsucht und diese auf Wunsch entfernt.

Zum komfortablen Einsatz von Virensclanner, Firewall und Anti-Spyware bieten mehrere Hersteller einen Komplettschutz in einem Programm an. Der Einsatz sowie Einstellungsmöglichkeiten solcher Programme werden im nachfolgenden Kapitel behandelt.

Auch die Verwendung alternativer Software für Ihre tägliche Internetkommunikation kann die Probleme durch Cookies und unerwünschte Softwareinstallation eventuell eindämmen, da alternative Software möglicherweise über bessere Sicherheitsmechanismen zur Abwehr derartiger Probleme verfügt.

Der beste Schutz bleibt allerdings nach wie vor Ihre Vorsicht beim Besuch von Websites und bei der Installation neuer Software bzw. beim Bestätigen von Dialogboxen.

5.6 Pharming

In einer gemeinsamen oder kombinierten Angriffsmethode nutzt das Verfahren des Pharmings die vielfältigen Eigenschaften von Viren, Würmern, Ad-/Spyware und Browser Hijacking. Damit Pharming erfolgreich sein kann, müssen bestimmte Dateien auf dem Computer manipuliert werden. Diese Dateien, unter anderem die Host-Datei, werden im Vorfeld durch einen Virus oder ein trojanisches Pferd überschrieben.


Wird im Browser eine Webadresse eingegeben, durchsucht der Computer in erster Linie die eigenen in der sogenannten Host-Datei gespeicherten Einträge danach, ob die angefragte Webseite bereits besucht wurde. Befindet sich in der Host-Datei ein Eintrag für die gesuchte Webseite, wird die Webseite direkt angewählt. Erfolgt keine Ermittlung der angefragten Seite, wird diese Anfrage an den DNS-Server (Domain Name Server) weitergeleitet. Nachfolgend führt der DNS-Server die Weiterleitung zum entsprechenden Speicherort der gesuchten Webseite durch.

Erfolgt hingegen ein Pharming-Angriff, wird primär die lokal auf dem Computer gespeicherte Host-Datei durch Malware manipuliert. Infolgedessen werden alle Anfragen automatisch auf gefälschte Webseiten weitergeleitet, obwohl die angegebene Adresse richtig geschrieben wurde. Eine weitere Verfahrensweise für Pharming ist das sogenannte DNS-Flooding, bei dem ein korumpierter DNS-Server die aktuelle Webanfrage auf einen anderen Server umleitet, obwohl auch hier der Benutzer die richtige Webadresse angewählt hat.

In beiden Fällen wird der User wie beim Phishing auf eine täuschend echt wirkende Internetseite umgeleitet, deren hauptsächliches Ziel es ist, Bankdaten in Form von PINs und TANs sowie Kreditkartendaten auszuspionieren.

5.7 Übung

Schadsoftware

Level		Zeit	ca. 15 min
Übungsinhalte	<ul style="list-style-type: none"> ✓ Verstehen, welche Gefahren es im Internet gibt ✓ Verstehen, welche Viren- und Wurmtypen aktiv sind ✓ Verstehen, was Ad-/Spyware und Pharming bedeuten 		
Übungsdatei	--		
Ergebnisdatei	<i>Schadsoftware.pdf</i>		

1. Was kann unter dem Begriff „Cyber-Mobbing“ verstanden werden?

a	Der virtuelle Diebstahl von Daten
b	Spionagesoftware
c	Die Verbreitung pornografischer oder extremistischer Inhalte im Internet
d	Das Verbreiten falscher oder boshafter Behauptungen im Internet
e	Personen dahin gehend manipulieren, dass sie Bankdaten offenlegen
f	Angriffe mit Viren und Würmern

2. Welche Aussagen treffen auf einen Virus zu?

a	Ein Virus ist ein Programm, das sich selbst vervielfältigt.
b	Ein Virus infiziert noch nicht infizierte Dateien mit seinem Schadcode.
c	Ein Virus ist genauso aufgebaut wie ein Wurm.

3. Aus welchen Bestandteilen setzt sich der Grundbauplan eines Virus zusammen? Nennen Sie die richtigen Komponenten.

a	Tarnung
b	Erkennung
c	Nutzlast
d	Infektion
e	Umprogrammierung
f	Löschen

4. Welche Typen von Viren gibt es?

a	Bootsektorviren
b	Prozessorviren
c	Speicherresidente Viren
d	Dateiviren
e	Explorer-Viren
f	Makro- und Skriptviren

5. Was trifft auf Würmer zu?

a	Würmer sind Viren.
b	Würmer müssen wie Viren vom Benutzer gestartet werden.
c	Würmer führen ein Eigenleben.
d	Würmer vermehren sich selbstständig.

6. Welche dieser Aussagen trifft auf Adware oder Spyware zu?

a	Ausschließlich Spyware sammelt Daten über den Benutzer.
b	Der Begriff „Adware“ steht für Software, die kostenlos ist und sich über Werbeeinblendungen finanziert.
c	Adware reinigt den Computer von Spyware.

7. Unter Pharming kann Folgendes verstanden werden.

a	Mails mit Werbung für pharmazeutische Produkte
b	Ein Onlinecomputerspiel
c	Das Weiterleiten einer Suchanfrage auf eine gefälschte Webseite

6

Schutz vor Viren und Malware

6.1 Antivirenprogramme verwenden

Um sich vor unerwünschten Manipulationen schützen zu können, empfiehlt es sich, auf jeden Fall neben regelmäßigen Updates des Betriebssystems, Updates des Browsers, der Plug-Ins und Apps, ein Antivirenprogramm auf Computern, Tablets, Smartphones und Mobiltelefonen zu installieren. Verwenden Sie zudem nie veraltete Software, da diese neben Inkompatibilität (nicht mehr unterstützte und nicht mehr funktionierende Software, die beispielsweise noch unter Windows XP funktionierte) auch anfälliger für Malware ist oder Sicherheitslücken enthält, die vielleicht durch Updates behoben wurden. Gerade Sicherheitslücken machen Systeme angreifbar gegenüber Hackerangriffen.

Alle diese Programme haben gemeinsam, dass sie auf sogenannte Virendatenbanken bzw. Virensignaturen zugreifen, die aufgrund der Schnelllebigkeit des Virenbestandes ständig auf dem neuesten Stand gehalten werden müssen. Achten Sie deshalb darauf, dass Sie Ihr Antivirenprogramm regelmäßig (am besten täglich) updaten.

- ✓ Erzeugen Sie falls möglich während oder nach der Installation des Antivirenprogramms ein Notfallspeichermedium. Mit ihm können Sie einen infizierten Computer starten, ohne dass ein Bootvirus unbemerkt in den Arbeitsspeicher geladen wird. Zusätzlich zu den Systemdateien befinden sich auf einem Notfallspeichermedium eine Start- und eine Prüfroutine des Antivirenprogramms, das in den meisten Fällen nach dem Booten des Computers startet.

Nahezu alle Antivirenprogramme haben eine Funktion, mit der von der Webseite des Herstellers ein Update der Virendatenbank auf Ihren Computer, Ihr Tablet oder Smartphone geladen wird. Bei den meisten Programmen erfolgt dieser Vorgang bei bestehender Internetverbindung automatisch, also ohne eine vorherige Anfrage.



Wenn es sich jedoch um Viren handelt, die in gepackter und gegebenenfalls auch verschlüsselter Form in den Computer gelangen, besteht die Gefahr, dass diese nicht oder nur unzureichend vom Virens Scanner erkannt werden. Diese Dateien haben meist Endungen wie *zip*, *rar*, *cab* etc. Auch neue Viren werden nicht immer zuverlässig erkannt, obwohl nahezu alle Antivirenprogramme nicht nur nach Viren, sondern auch nach bekannten Verhaltensmustern von Viren suchen (Heuristik). So werden auch Viren, die nicht in der Virenliste stehen, erkannt.

Sollte Ihr Virens Scanner nicht die Erstellung eines Notfallspeichermediums ermöglichen, erhalten Sie weitere Informationen zur Anwendung und die Möglichkeit des Downloads einer Rettungs-CD unter www.botfrei.de/rescuecd.html.

6.2 Erste Schritte bei einer Vireninfektion

Auch der sorgsamste Anwender kann nicht ausschließen, dass sich irgendwann ein Virus in seinen Computer oder in sein mobiles Gerät einschleust. Das Vorhandensein eines Virus erkennen Sie entweder am anormalen Verhalten des Computers (er versucht z. B. im Hintergrund, eine Internetverbindung herzustellen, Systemfunktionen können nicht mehr aufgerufen werden etc.) oder einer entsprechenden Meldung, die der Virus selbst oder aber das Antivirenprogramm ausgibt. Einen größeren Schaden als der Virus selbst richtet oft die übertriebene Reaktion auf ihn an. Oft werden im ersten Schrecken Dateien bzw. Programme gelöscht oder es wird sogar die Festplatte formatiert, obwohl der Virus sich zwar lokal eingenistet, aber bisher keinen Schaden verursacht hat.

- ✓ Ist Ihr Computer mit dem Internet verbunden, trennen Sie sofort die Verbindung, notfalls durch Abziehen des Kabels.
- ✓ Fahren Sie den Computer herunter.
- ✓ Starten Sie ihn von dem schreibgeschützten Notfallspeichermedium (Boot-CD mit installiertem Antivirenprogramm) oder von einem entsprechenden bootfähigen USB-Stick.

Wird nach dem Start mit einem Notfallspeichermedium die Festplatte nicht mehr erkannt, müssen Sie den Computer noch einmal über die Festplatte starten. Nehmen Sie dazu das Speichermedium aus dem Laufwerk. Der Virus hat die Partitionstabelle so verändert, dass die Partitionen der Festplatte nur mit dem Virus erkannt werden. Sichern Sie die wichtigsten Dateien, die Sie auf anderem Wege nicht mehr wiederherstellen können, und führen Sie erneut einen Systemstart über das Notfallspeichermedium aus.

- ✓ Prüfen Sie Ihr System mit einem Antivirenprogramm und löschen bzw. reparieren Sie die infizierten Dateien mit dessen Hilfe.

Aktuelle Viren installieren in Kombination mit Botnetzen teilweise schädliche Software nach. Unter einem Botnetz versteht man dabei ein Netzwerk bestehend aus infizierten Computern, die ferngesteuert werden. Manche Antivirenprogramme entfernen nur die entsprechenden Viren – nicht jedoch die durch diese eingeschleuste Software. Gegebenenfalls ist deshalb eine Neuinstallation des Betriebssystems bzw. das Aufspielen eines „sauberen“ Backups erforderlich.

6.3 Virens Scanner installieren

Virens Scanner installieren

Als Virens Scanner können Sie neben vielen anderen sehr guten Virens Scannern beispielsweise den avast! Free Antivirus der Firma avast! Nutzen. Die Setup-Datei für Windows können Sie von der Webseite www.avast.com/de-de/index herunterladen.

Nachdem Sie die Installationsdatei auf Ihren Computer kopiert haben, können Sie avast! Free Antivirus installieren. Beachten Sie, dass kein anderes Antivirenprogramm installiert ist. Befinden sich mehrere Antivirenprogramme auf einem Computer, stören sie sich gegebenenfalls gegenseitig bei der Virensuche oder führen im schlimmsten Fall zum Absturz des Systems.

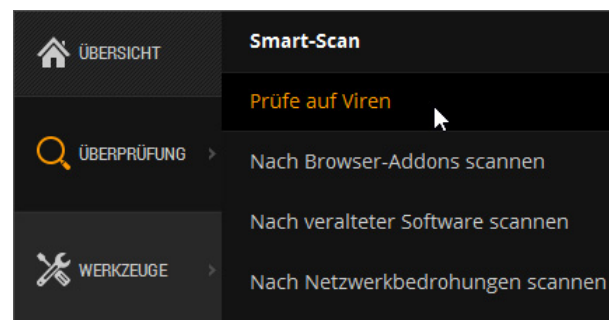
- ▶ Öffnen Sie den Ordner, in dem Sie die Setup-Datei gespeichert haben.
- ▶ Klicken Sie doppelt auf die Setup-Datei und folgen Sie den weiteren Installationsanweisungen.

6.4 Einstellungen für die Virensuche festlegen

Den Computer überprüfen

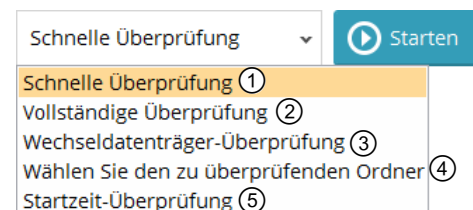
Standardmäßig werden alle Dateien auf Virenbefall kontrolliert. Sie können aber avast! Free Antivirus anweisen, die Überprüfung zu individualisieren.

- Klicken Sie im Navigationsbereich auf *Überprüfung* und auf *Prüfen auf Viren*.



Um eine Überprüfung ausgewählter Bereiche (z. B. Systemlaufwerk, Festplatten, Autostart-Programme oder im Speicher geladene Module) durchzuführen sowie nach Rootkits zu suchen, gehen Sie wie folgt vor:

- Wählen Sie einen Eintrag ①–④ aus und klicken Sie auf *Starten*.




Nach erfolgreicher Beendigung der Suche wird ein Bericht über das Ergebnis eingeblendet.

Wenn Sie den Eintrag ⑤ auswählen und auf *Einstellungen* klicken, können Sie eine Überprüfung ausgewählter Bereiche für den nächsten Systemstart planen. Schließen Sie die Einstellungen mit einem Klick auf *OK* ab.

Einstellmöglichkeiten

Alternativ können Sie die Überprüfung auch individualisieren.

- Wählen Sie einen Eintrag ①–④ aus und klicken Sie auf *Einstellungen*.

Prüfungs-einstellung	Definition
Überprüfung	✓ Dies sind schreibgeschützte Einstellungen, die nicht geändert werden können.
Wirkungsgrad	<ul style="list-style-type: none"> ✓ Der Heuristik-Einsteller  gibt den Wirkungsgrad der Suche an. ✓ Wird das Kontrollfeld <i>Code-Emulation verwenden</i> aktiviert, wird potenziell gefährlicher Code in einer virtuellen Umgebung überprüft, ohne dass der PC geschädigt wird. ✓ Die Aktivierung des Kontrollfelds im Bereich <i>Wirkungsgrad</i> bewirkt die Überprüfung sämtlicher Dateien. ✓ Aktivieren Sie das Kontrollfeld <i>Auf potentiell unerwünschte Programme (PUP) prüfen</i>, um auf Programme zu prüfen, bei denen die Gefahr besteht, dass personenbezogene Daten ohne Ihr Wissen an Dritte übermittelt werden.
Archive (Packer)	✓ Aktivieren Sie hier das Kontrollfeld <i>Alle Packer</i> oder differenzieren Sie die Auswahl der zu überprüfenden Packerformate.

Prüfungseinstellung	Definition
Aktionen	<ul style="list-style-type: none"> ✓ Standardmäßig ist hier keine Aktion, die nach der Überprüfung durchgeführt wird, hinterlegt. Definieren Sie durch Aktivieren des Kontrollfelds <i>Aktionen automatisch während der Überprüfung durchführen</i>, welche Aufgaben durchgeführt werden sollen. ✓ Regeln Sie im Bereich <i>Optionen</i>, wie mit infizierten Archiven umzugehen ist.
Leistung	<ul style="list-style-type: none"> ✓ Nutzen Sie den Einsteller <i>Priorität</i>, um die benötigte Zeit und den Speicherplatz anzupassen. Die Priorität <i>Hoch</i> kann eine hohe Prozessorauslastung bewirken. ✓ Unterscheiden Sie im Bereich <i>Beständige Zwischenspeicherung</i>, ob die Speicherung von Informationen bereits geprüfter Dateien die Überprüfungsgeschwindigkeit erhöhen soll (<i>aktiviert</i>) oder ob Daten der geprüften Dateien im beständigen Zwischenspeicher abgespeichert werden sollen.
Protokolldatei	<ul style="list-style-type: none"> ✓ Aktivieren Sie das Kontrollfeld <i>Berichtdatei erstellen</i>, um einen Dateinamen und -typ festzulegen sowie die Berichtseinstellungen zu definieren.
Ausnahmen	<ul style="list-style-type: none"> ✓ Legen Sie die Pfade fest, die nicht überprüft werden sollen.
Zeitplan	<ul style="list-style-type: none"> ✓ Aktivieren Sie das Kontrollfeld <i>Zeitplan festlegen</i>, um eine automatische Überprüfung zu planen.

6.5 Datenträger gezielt auf Viren überprüfen

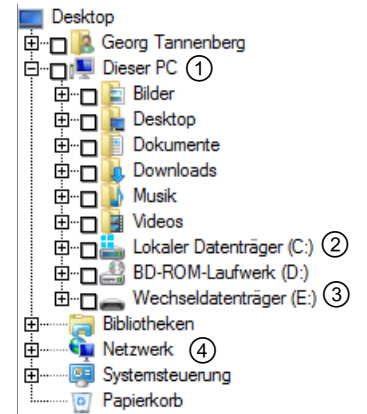
Zu durchsuchende Laufwerke festlegen

Wenn Sie Laufwerke und Ordner auf einen möglichen Virenbefall untersuchen möchten, starten Sie den Scan mit dem Eintrag *Wählen Sie den zu überprüfenden Ordner* und *Starten*.

Sie können den Suchbereich gezielt auf bestimmte Laufwerke einschränken, beispielsweise wenn Sie fremde Dateien von einer CD oder einem Wechseldatenträger (USB-Stick) auf Ihren Computer kopieren möchten und nicht sicher sind, ob diese Dateien Viren enthalten.

- Klicken Sie im Bereich *Wählen Sie den zu überprüfenden Ordner* auf *Starten*.
oder Klicken Sie vorher auf *Einstellungen*, um die bereits beschriebenen Einstellungen vorzunehmen.

- ▶ Aktivieren Sie das Kontrollfeld ①, um den gesamten Computer zu überprüfen.
- oder* Aktivieren Sie das Kontrollfeld ② oder ③, um ein einzelnes Laufwerk oder ein Netzlaufwerk auf Viren zu kontrollieren.
- oder* Klicken Sie doppelt auf ④, um einen im Netzwerk eingebundenen PC auf Viren zu überprüfen.
- ▶ Klicken Sie abschließend auf **OK**, um den Suchvorgang zu starten.

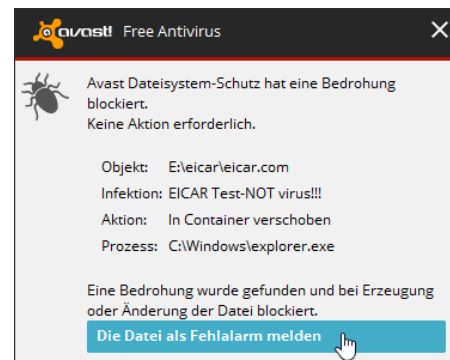


6.6 Auf gefundene Viren reagieren

Mit infizierten Dateien umgehen

Findet avast! Free Antivirus einen Virus auf Ihrem Computer, wird ein Warndialog eingeblendet. Gehen Sie wie folgt vor:

- ✓ Falls es sich bei der Meldung um einen Fehlalarm handelt, übermitteln Sie dies avast! durch einen Klick auf den Link *Die Datei als Fehlalarm melden*.
- ✓ Tätigen Sie weitere Schritte, wie im folgenden Abschnitt beschrieben.
- ✓ In Quarantäne gestellte Dateien werden verschlüsselt und in einen entsprechenden Ordner verschoben, sodass sie keine weiteren Schäden verursachen können.



In Quarantäne gestellte Dateien behandeln

avast! Free Antivirus zeigt standardmäßig bei einem Virenfund den zuvor beschriebenen Warndialog an und verschiebt Dateien in den Virus Container. Dateien, die in die Quarantäne verschoben wurden, können Sie wie folgt behandeln:

- ▶ Klicken Sie auf *Überprüfung* und im unteren Bereich auf den Link *Quarantäne (Virus Container)*.
- ▶ Klicken Sie mit der rechten Maustaste auf die gewünschte Datei und führen Sie eine unten beschriebene Aktion durch Anklicken aus.



Vorgang	Beschreibung
Löschen	<ul style="list-style-type: none"> ✓ Bevor Sie eine infizierte Datei löschen, überprüfen Sie, ob ein Backup oder eine Installations-CD mit der entsprechenden nicht infizierten Datei vorhanden ist. ✓ Führen Sie vor dem Löschen oder der Reparatur einer infizierten Datei eine Sicherung wichtiger Dateien durch, notfalls auch infizierter Dateien. ✓ Wird durch die Reparatur die Datei zerstört, können Sie abwägen, ob Sie die Daten auf einem infizierten Computer noch drucken bzw. in Teilen kopieren. Dabei sollte jedoch auf jeden Fall die Internet-Verbindung gekappt sein. ▶ Klicken Sie im Kontextmenü auf <i>Löschen</i>. ▶ Klicken Sie im geöffneten Fenster auf <i>Ja</i>, um die Datei endgültig zu löschen.
Wiederherstellen	<ul style="list-style-type: none"> ▶ Klicken Sie im Kontextmenü auf <i>Wiederherstellen</i>, um die ggf. noch infizierte Datei an ihren Ursprungsort zu kopieren.
Aus Container extrahieren	<ul style="list-style-type: none"> ▶ Klicken Sie auf <i>Aus Container extrahieren</i>, um die Datei an einen neuen Speicherort zu kopieren.
Überprüfung	<ul style="list-style-type: none"> ▶ Klicken Sie auf <i>Überprüfen</i>, um die sich in Container befindende Datei nochmals auf Viren zu überprüfen.
An das Virenlabor übermitteln	<ul style="list-style-type: none"> ▶ Klicken Sie im Kontextmenü auf <i>An das Virenlabor übermitteln</i>, um die gefundene Virenstruktur zur Analyse an den Hersteller zu senden. ▶ Machen Sie im Fenster <i>Datei senden</i> die benötigten Angaben und aktivieren Sie das Kontrollfeld <i>Ich weiß was ich tue</i>. ▶ Klicken Sie abschließen auf <i>Übermitteln</i>.
Eigenschaften	<ul style="list-style-type: none"> ▶ Klicken Sie im Kontextmenü auf <i>Eigenschaften</i>, um mehr über die Dateieigenschaften zu erfahren.
Hinzufügen	<ul style="list-style-type: none"> ▶ Klicken Sie auf <i>Hinzufügen</i>, um manuell weitere Dateien in den Container zu laden.
Alle Dateien aktualisieren	<ul style="list-style-type: none"> ▶ Durch Klicken auf <i>Alle Dateien aktualisieren</i> wird der im Container befindliche Datenstamm aktualisiert.

Durch das Markieren von mehreren Dateien, die sich im Virus Container befinden, können Sie einen ausgewählten Vorgang auf alle Dateien anwenden.

6.7 PC vor Spyware und Botnetzen schützen

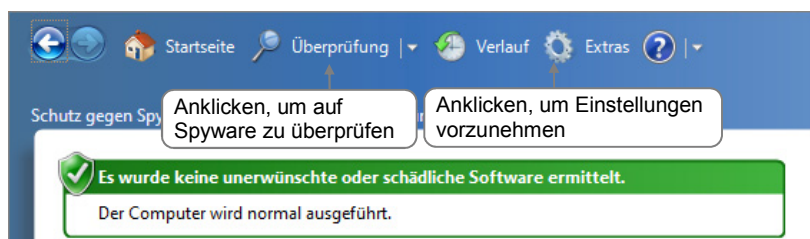
Den PC mit Windows Defender wieder benutzbar machen

Sind auf einem PC erst einmal zweifelhafte Programme installiert worden, bleiben diese in der Regel nicht lange allein. Entweder werden aufgrund des Surfverhaltens des Benutzers weitere Schadprogramme installiert oder die bereits installierte Schadsoftware installiert heimlich weitere Software nach. Analog zu Virenscannern, die größtenteils auch vor Spyware und Botnetzen schützen, gibt es auf dem Markt zahlreiche Produkte, die es sich zur Aufgabe gemacht haben, einen befallenen PC von Spyware, beispielsweise von Cookies, zu befreien.

Windows Defender schützt wie viele Virenscanner vor Spyware und unerwünschten Programmen. Er ist Bestandteil von Windows 7–10.

Windows Defender unter Windows 7 nutzen

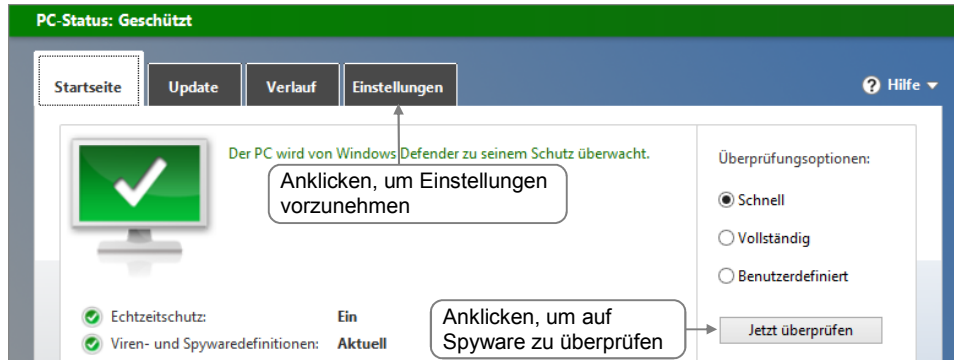
- ▶ Klicken Sie auf die Startschaltfläche von Windows 7.
- ▶ Geben Sie im Suchfeld von Windows 7 die Anfangsbuchstaben des Programmnamens (*defe*) ein und wählen Sie in der anschließend eingeblendeten Liste *Windows Defender*.



- ▶ Klicken Sie auf *Extras* und wählen Sie im Bereich *Optionen* den Eintrag *Automatische Überprüfung*, um die Häufigkeit, die geschätzte Zeit und den Typ der regelmäßigen Überprüfung einzustellen.
oder Wählen Sie den Eintrag *Erweitert* und aktivieren Sie das Kontrollfeld *E-Mail überprüfen*, um im Rahmen der Überprüfung das E-Mail-Postfach einzubinden.
- ▶ Beenden Sie die Einstellungen durch Klick auf *Speichern*.

Windows Defender unter Windows 8.1 und Windows 10 einsetzen

- ▶ Tragen Sie auf dem Startbildschirm von Windows 8.1 das Wort *defender* ein und klicken Sie auf *Windows Defender*.
oder Geben Sie nach einem Klick auf die Startschaltfläche von Windows 10 im Suchfeld die Anfangsbuchstaben des Programmnamens (*defe*) ein und klicken Sie auf *Windows Defender*.

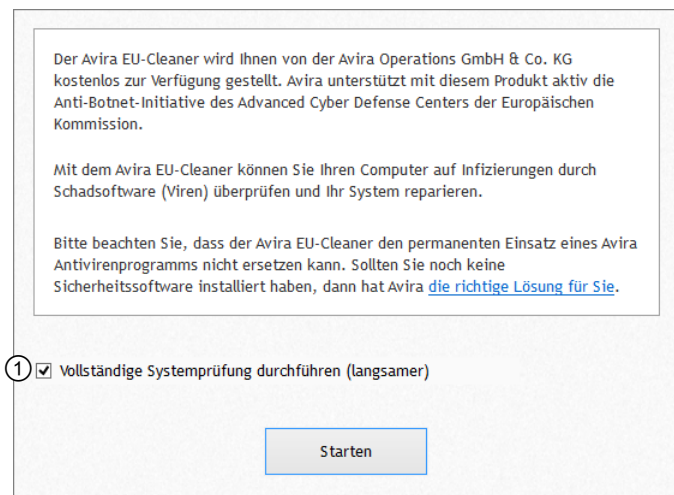


Nach Botnetzen suchen

Zusätzlich zu den bereits bekannten Methoden, Spyware und Botnetze zu erkennen und zu entfernen, gibt es auch Online-Ressourcen (Webseiten des Betriebssystems, Online-Anti-Virus-Software) sowie Webseiten entsprechender Behörden, wie das Bundesamt für Sicherheit in der Informationstechnik, wo Sie unter www.botfrei.de/eucleaner.html verschiedene Programme zum Aufspüren und Entfernen von schädlicher Software erhalten.

Als Beispiel dient hier der von Symantec vertriebene EU-Cleaner.

- ▶ Klicken Sie unter www.botfrei.de/eucleaner.html auf *EU-Cleaner powered by Avira* und folgen Sie den weiteren Anweisungen zum Download.
- ▶ Klicken Sie doppelt auf die Datei *avira-eu-cleaner_de*, um sie auszuführen.
Der Cleaner wird heruntergeladen.
- ▶ Klicken Sie auf *Akzeptieren*.
- ▶ Klicken Sie im Fenster *Benutzerkontensteuerung* auf *Ja*.
- ▶ Aktivieren Sie das Kontrollfeld ①, damit der Computer vollständig überprüft wird.
- ▶ Klicken Sie auf *Starten*, um den Scanvorgang einzuleiten.
- ▶ Klicken Sie auf *Weiter* und wählen Sie *Nicht senden*.
- ▶ Beenden Sie den Vorgang mit Klick auf *OK*.



7

Sicher im Internet arbeiten

7.1 Sicherheitsoptionen im Internet Explorer

Die folgende Tabelle stellt eine Übersicht der vom Internet Explorer 10–Internet Explorer 11 angebotenen Sicherheitsoptionen dar.

Sicherheitsprotokolle	Ein Sicherheitsprotokoll gewährleistet eine sichere, nicht abhörbare Verbindung mit der entsprechenden Webseite. Hierzu werden die ein- bzw. ausgehenden Daten kodiert (verschlüsselt). Der Internet Explorer erkennt, ob eine Webseite mit einem Sicherheitsprotokoll arbeitet und stellt dies in der Adressleiste dar.
Sicherheitszertifikate bzw. digitale Zertifikate	Ein Sicherheitszertifikat bzw. ein digitales Zertifikat ist eine Art elektronischer Ausweis, der weitgehend fälschungssicher ist und die Identität einer Webseite oder einer Person bestätigt (Authentifizierung). Zertifikate werden nur durch autorisierte Zertifizierungsstellen ausgestellt.
Sicherheitszonen	Im Internet Explorer 10 und Internet Explorer 11 lassen sich Webseiten Sicherheitszonen mit unterschiedlichen Sicherheitsstufen zuordnen. So können Sie beispielsweise durch die Zuordnung zur Sicherheitszone <i>Eingeschränkte Sites</i> festlegen, dass Seiten, denen Sie nicht vertrauen, keine aktiven Inhalte (z. B. sogenannte ActiveX-Steuerelemente) ausführen dürfen. Aktive Inhalte können ohne Ihre Zustimmung beispielsweise Computereinstellungen verändern oder Programme installieren.
Datenschutzeinstellungen für Cookies festlegen	Sie können für die vorhandenen Sicherheitszonen bestimmte Datenschutzeinstellungen festlegen, um die Behandlung von Daten zu regeln, die der Browser im Auftrag von bestimmten Webseiten auf der Festplatte zu speichern versucht (sogenannte Cookies).

Der Internet Explorer warnt standardmäßig, wenn eine Webseite bzw. eine von Ihnen eingeleitete Aktion bestimmte Sicherheitsrisiken birgt (z. B. wenn Zweifel an der Echtheit des verwendeten Sicherheitszertifikats bestehen).

Unter folgenden Internetadressen erhalten Sie aktuelle Informationen/Tipps zum Thema „Datensicherheit“:

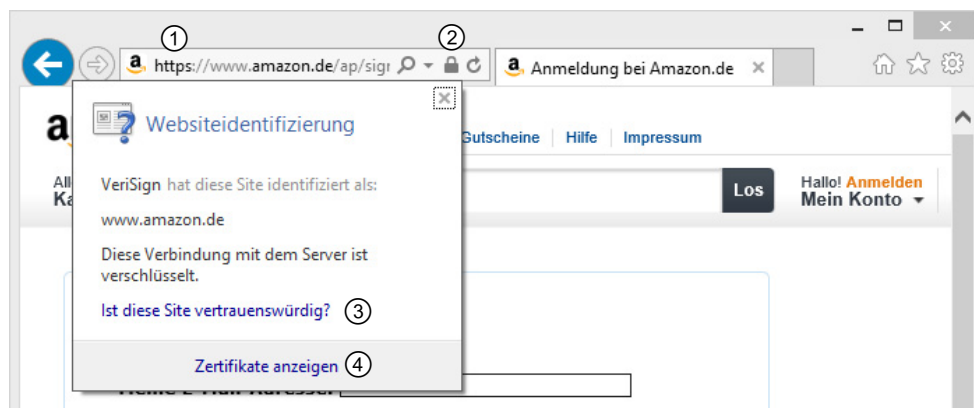
- ✓ www.saferinternet.at
- ✓ www.a-sit.at
- ✓ www.heise.de/security

7.2 Sicherheitsprotokolle und -zertifikate erkennen

Webseiten mit Sicherheitsprotokollen und -zertifikaten identifizieren

Möchten Sie über das Internet bestellen oder einkaufen und dabei persönliche Daten wie Adresse und Kontoverbindung/Kreditkartendaten übertragen, sollten Sie darauf achten, dass die Webseite, die diese Daten von Ihnen anfordert, mit einem Sicherheitsprotokoll arbeitet. So stellen Sie (weitgehend) sicher, dass beim Übertragen der Daten keine Unbefugten an die entsprechenden Informationen gelangen können.

Die meisten Webseiten nutzen zur sicheren Datenübertragung das Sicherheitsprotokoll **Secure Socket Layer (SSL)**, das den Aufbau eines abgesicherten Kommunikationskanals zur Webseite ermöglicht. Sie erkennen das Protokoll in der Adressleiste am Präfix **https** ① und am Schlosssymbol ②. Durch Anklicken des Schlosssymbols können Sie sich die Eigenschaften des zugehörigen Zertifikats anzeigen lassen.



- ✓ Über den Link ③ können Sie die Hilfe aufrufen. Sie erhalten dort weitere Informationen zum Thema „Vertrauenswürdige Webseiten“.
- ✓ Nähere Informationen zum Zertifikat erhalten Sie, indem Sie auf den Link ④ klicken.

! Wissen Sie nicht genau, ob es sich um eine „sichere“ Verbindung handelt, sollten Sie **keinesfalls** Kreditkarteninformationen, Kontoangaben oder persönliche Daten angeben. Fragen Sie stattdessen telefonisch oder per E-Mail beim Betreiber der Webseite nach, ob bzw. wie Sie die Informationen verschlüsselt senden können oder ob eventuell andere Zahlungsmodalitäten zur Verfügung stehen.

Verwendetes Zertifikat anhand der Farbe der Adressleiste beurteilen

Anhand der Farbe der Adressleiste können Sie erkennen,

- ✓ ob das angegebene Zertifikat gültig ist,
- ✓ wie die betreffende Webseite durch die Zertifizierungsstelle geprüft wurde.

Farbe	Bedeutung
Grün	Die Kommunikation zwischen dem Internet Explorer und der aufgerufenen Webseite ist verschlüsselt. Zusätzlich wird von der Zertifizierungsstelle bestätigt, dass sich der Betreiber der Webseite zur Einhaltung der Sicherheits- und Rechtsbestimmungen des angegebenen Zertifikats verpflichtet hat (erweiterte Prüfung).
Weiß	Die Kommunikation zwischen dem Internet Explorer und der aufgerufenen Webseite ist verschlüsselt (normale Prüfung).
Gelb	Es kann nicht überprüft werden, ob das Zertifikat gültig ist.
Rot	Es wurde ein Zertifikatsfehler festgestellt: Das angegebene Zertifikat ist ungültig, nicht mehr gültig oder weist Fehler auf.

Wenn Sie zu einer Webseite wechseln, bei der das Zertifikat ungültig ist bzw. nicht anerkannt wird, erhalten Sie eine sogenannte Zertifikatsfehlermeldung.

Es besteht ein Problem mit dem Sicherheitszertifikat der Website.

Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.

Die Sicherheitszertifikatsprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.

Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.

① [Klicken Sie hier, um diese Webseite zu schließen.](#)

② [Laden dieser Website fortsetzen \(nicht empfohlen\).](#)

[Weitere Informationen](#)

- ✓ Möchten Sie das Laden der Webseite abbrechen, klicken Sie auf den Link ① und bestätigen Sie die anschließende Rückfrage mit *Ja*. Der Internet Explorer wird dadurch geschlossen.
- ✓ Nur wenn Sie sich absolut sicher sind, dass Sie die Webseite trotz erfolgter Zertifikatsfehlermeldung laden möchten, klicken Sie auf den Link ②. Die gewählte Webseite wird geöffnet und die Adressleiste wird rot hinterlegt. Bis zu einem erneuten Start des Internet Explorers erhalten Sie in diesem Fall keine weitere Fehlermeldung über das fehlerhafte Zertifikat.



Rot hinterlegte kombinierte Adressleiste mit Zertifikatsfehler

7.3 Echtheit einer Webseite überprüfen

Die Echtheit einer Webseite können Sie anhand verschiedener Kriterien überprüfen.

- ✓ Qualität und Aktualität des Inhaltes
- ✓ Gültige URL
- ✓ Impressum (Unternehmens- oder Eigentümerinformationen)
- ✓ Kontaktinformationen
- ✓ Sicherheitszertifikat

Neben den genannten Kriterien spielt auch die Validierung des Domaininhabers eine große Rolle. Informationen über die Domain bzw. über den Domaininhaber erhalten Sie bei der entsprechenden zentralen Registrierungsstelle für Top-Level-Domains, z. B. für AT-Domains bei der nic.at GmbH (www.nic.at).

7.4 Sicherheitszonen für Webseitenutzen

Wozu dienen Sicherheitszonen?

Im Internet Explorer existieren vier Sicherheitszonen (vgl. folgende Tabelle), die jeweils unterschiedliche Sicherheitseinstellungen (Sicherheitsstufen) aufweisen. Standardmäßig sind sämtliche Webseiten zunächst der Sicherheitszone *Internet* zugeordnet, für die die Sicherheitsstufe *Mittel bis hoch* voreingestellt ist.

Sie können bei Bedarf bestimmte Webseiten einer anderen Sicherheitszone zuweisen, damit diese mit anderen Sicherheitseinstellungen ausgeführt werden. Wenn Sie beispielsweise eine Webseite, der Sie nicht vertrauen, der Sicherheitszone *Eingeschränkte Sites* zuordnen, kann diese Seite keine aktiven Inhalte (z. B. sogenannte ActiveX-Steuerelemente oder Java-Script-Applets) ausführen. Aktive Inhalte können ohne Ihre Zustimmung beispielsweise Computereinstellungen verändern oder Programme installieren.

Sicherheitszone	Erläuterung
<i>Internet</i> (Sicherheitsstufe <i>Mittel bis hoch</i>)	Diese Sicherheitszone beinhaltet automatisch alle Webseiten des Internets, die nicht manuell einer anderen Zone zugeordnet wurden.
<i>Lokales Intranet</i> (Sicherheitsstufe <i>Niedrig</i>)	In dieser Sicherheitszone befinden sich alle Webseiten Ihres lokalen Firmennetzes. Die entsprechenden Webseiten werden dieser Zone vom Systemadministrator zugeordnet.
<i>Vertrauenswürdige Sites</i> (Sicherheitsstufe <i>Mittel</i>)	Dieser Zone können Sie alle Webseiten zuweisen, denen Sie vertrauen, d. h., die Ihrer Meinung nach keine Gefahr für Ihren Rechner darstellen.
<i>Eingeschränkte Sites</i> (Sicherheitsstufe <i>Hoch</i>)	Weisen Sie dieser Zone alle Webseiten zu, denen Sie nicht vertrauen, da sie eventuell eine Gefahr für Ihren Rechner sind. Da in dieser Zone die Ausführung aktiver Inhalte verhindert wird, kann es ggf. vorkommen, dass die betreffenden Webseiten nicht richtig dargestellt werden.

Alle Webseiten, die den Sicherheitszonen *Internet*, *Lokales Intranet* bzw. *Eingeschränkte Sites* zugeordnet wurden, zeigt der Internet Explorer im sogenannten **geschützten Modus** an. In diesem Modus warnt Sie der Browser mit entsprechenden Hinweisen, wenn Webseiten versuchen, Programme zu installieren bzw. auszuführen.

7.5 Datenschutzeinstellungen für Cookies ändern


Was sind Cookies?

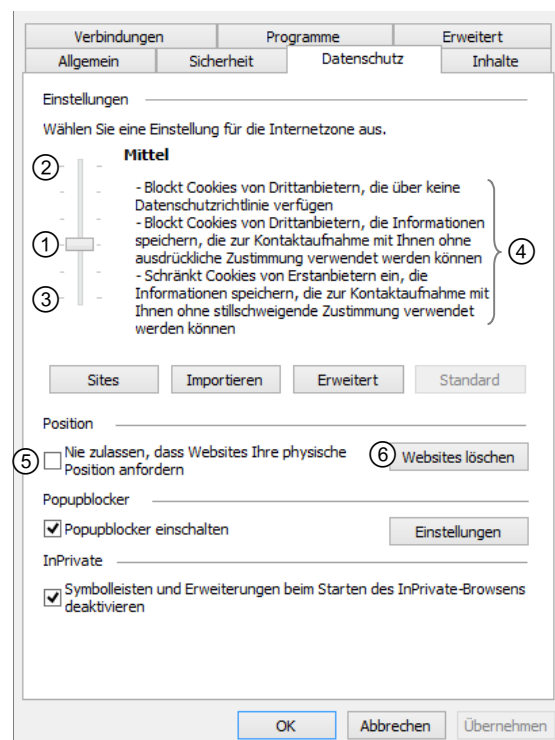
Cookies (engl. Ausdruck für Plätzchen oder Kekse) sind Dateien, in denen der Browser Benutzerdaten und -einstellungen im Auftrag des Webserver der besuchten Webseite im Ordner für temporäre Internetdaten auf dem Rechner des Besuchers speichert.

Beim erneuten Besuch der Webseite können diese Daten vom Browser an den Webserver übertragen und ausgewertet werden. Diese Daten sollen beispielsweise bei späteren Sitzungen helfen, den Anwender individuell „bedienen“ zu können. Allerdings können hierbei auch persönliche Daten über Ihr Nutzerverhalten gespeichert werden, die dann anderen Personen zur Verfügung stehen.

Individuelle Einstellungen für Cookies festlegen

Sie können im Fenster *Internetoptionen* festlegen, welche Einstellungen der Internet Explorer für Cookies in der Sicherheitszone *Internet* verwenden soll.

- ▶ Klicken Sie neben der Adressleiste auf , wählen Sie *Internetoptionen* und aktivieren Sie im geöffneten Fenster *Internetoptionen* das Register *Datenschutz*.
- ▶ Stellen Sie mithilfe des Schiebereglers ① die gewünschte Cookie-Behandlung ein.
 - ✓ Möchten Sie z. B., dass das Speichern und Lesen von Cookies generell verhindert wird, wählen Sie *Alle Cookies blocken* (Schiebereglerposition ②). Sollen alle Cookies gespeichert und von den Webseiten, die sie gesetzt haben, auch wieder gelesen werden dürfen, wählen Sie *Alle Cookies annehmen* (Position ③).
 - ✓ Die Auswirkungen der jeweils gewählten Einstellung werden im Bereich ④ kurz erläutert.
- ▶ Betätigen Sie *Sites*, um für einzelne Webseiten gezielt eine bestimmte Cookie-Behandlung festzulegen.
- ▶ Bestätigen Sie mit *OK*.





Über *Erweitert* können Sie die automatische Cookie-Behandlung aufheben und bei Bedarf generelle Einstellungen für die Cookie-Behandlung manuell festlegen, beispielsweise um Cookies sogenannter Drittanbieter (z. B. Werbeanzeigen, die von einem anderen Server stammen) immer zu blocken. Die so getroffenen Einstellungen haben Vorrang gegenüber denen, die im Register *Datenschutz* festgelegt wurden.

Aktivieren Sie das Kontrollfeld ⑤, um eine mögliche Standortlokalisierung durch den Webseitenbetreiber zu deaktivieren. Klicken Sie des Weiteren auf die Schaltfläche ⑥, um alle zwischengespeicherten Webseiten zu löschen, die bereits Ihren Standort lokalisiert haben.

Temporäre Internetdateien löschen

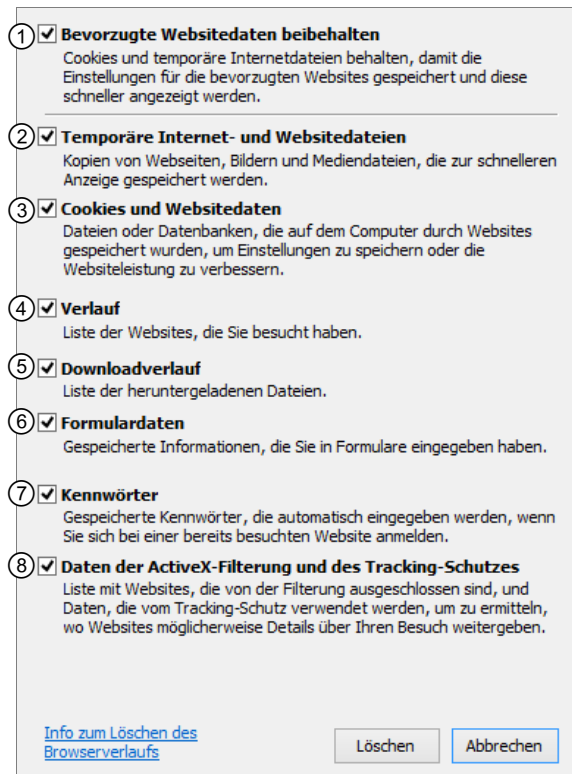
Standardmäßig speichert der Internet Explorer im Ordner für temporäre Internetdaten nicht nur Cookies, sondern beispielsweise auch Informationen zu besuchten Webseiten (z. B. dort vorhandene Icons etc.) bzw. Eingaben, die Sie in der Adressleiste bzw. auf einer Webseite getätigt haben.

Sie können die gespeicherten temporären Dateien folgendermaßen entfernen:

- ▶ Klicken Sie neben der Adressleiste auf , wählen Sie *Sicherheit* und klicken Sie auf *Browserverlauf löschen*.
Alternative: **Strg**  **Entf**
- ▶ Nehmen Sie im geöffneten Fenster die gewünschten Einstellungen vor (vgl. folgende Erläuterungen).
- ▶ Bestätigen Sie mit der Schaltfläche *Löschen*.

Bei aktiviertem Kontrollfeld ...

- ① bleiben alle Cookies bzw. temporären Internetdateien erhalten, die zu Favoriten existieren.
- ② werden alle gespeicherten Elemente von Webseiten (z. B. Bilder und Icons) gelöscht – außer den entsprechenden Elementen der Favoriten, falls Sie das Kontrollfeld ① aktiviert haben.
- ③ werden alle gespeicherten Cookies gelöscht – außer den Cookies der Favoriten, falls Sie das Kontrollfeld ① aktiviert haben.
- ④ wird der komplette Browserverlauf (Liste der aufgerufenen Webseiten) gelöscht.
- ⑤ wird die Liste der bislang getätigten Downloads gelöscht.
- ⑥ werden die Formulardaten gelöscht, die mithilfe der Funktion *AutoVervollständigen* gespeichert wurden.
- ⑦ werden die Kennwörter gelöscht, die mithilfe der Funktion *AutoVervollständigen* gespeichert wurden.
- ⑧ werden alle Daten der ActiveX-Filterung und dem Tracking-Schutz gelöscht.



① ☒ **Bevorzugte Websitedaten beibehalten**
Cookies und temporäre Internetdateien behalten, damit die Einstellungen für die bevorzugten Websites gespeichert und diese schneller angezeigt werden.

② ☒ **Temporäre Internet- und Websitedateien**
Kopien von Webseiten, Bildern und Mediendateien, die zur schnelleren Anzeige gespeichert werden.

③ ☒ **Cookies und Websitedaten**
Dateien oder Datenbanken, die auf dem Computer durch Websites gespeichert wurden, um Einstellungen zu speichern oder die Websiteleistung zu verbessern.

④ ☒ **Verlauf**
Liste der Websites, die Sie besucht haben.

⑤ ☒ **Downloadverlauf**
Liste der heruntergeladenen Dateien.


⑥ ☒ **Formulardaten**
Gespeicherte Informationen, die Sie in Formulare eingegeben haben.

⑦ ☒ **Kennwörter**
Gespeicherte Kennwörter, die automatisch eingegeben werden, wenn Sie sich bei einer bereits besuchten Website anmelden.

⑧ ☒ **Daten der ActiveX-Filterung und des Tracking-Schutzes**
Liste mit Websites, die von der Filterung ausgeschlossen sind, und Daten, die vom Tracking-Schutz verwendet werden, um zu ermitteln, wo Websites möglicherweise Details über Ihren Besuch weitergeben.

[Info zum Löschen des Browserverlaufs](#)


Löschen **Abbrechen**

Sie können im Fenster *Internetoptionen* (, *Internetoptionen*) festlegen, dass der Browserverlauf automatisch beim Schließen des Internet Explorers gelöscht wird. Aktivieren Sie hierzu im Register *Allgemein* das Kontrollfeld *Browserverlauf beim Beenden löschen*.



7.6 Blockieren von Inhalten

Den Tracking-Schutz aktivieren

Viele Webseiten versuchen, personenbezogene Daten über Sie zu sammeln, um personalisierte Werbung einzublenden. Der im Internet Explorer 10 und Internet Explorer 11 integrierte Tracking-Schutz blockiert diesen Ladevorgang und schützt Sie vor unbeabsichtigter Weitergabe von Informationen.

- ▶ Klicken Sie neben der Adressleiste auf , wählen Sie *Sicherheit* und klicken Sie auf *Tracking-Schutz...*
- ▶ Klicken Sie im geöffneten Fenster *Add-Ons verwalten* auf *Tracking-Schutz* und auf *Liste für den Tracking-Schutz online abrufen...*
Im neu geöffneten Fenster haben Sie die Möglichkeit, verschiedene Tracking-Schutz-Listen zu Ihrem Schutz hinzuzufügen.
- ▶ Klicken Sie auf *Hinzufügen* und klicken Sie im geöffneten Fenster *Tracking-Schutz* auf *Liste hinzufügen*.

Eine personalisierte Tracking-Schutz-Liste anlegen

- ▶ Klicken Sie neben der Adressleiste auf , wählen Sie *Sicherheit* und klicken Sie auf *Tracking-Schutz...*
- ▶ Klicken Sie im Fenster *Add-Ons verwalten* auf *Tracking-Schutz* und dann auf den Listeneintrag *Ihre angepasste Liste*.
- ▶ Klicken Sie auf *Aktivieren* und danach auf die Schaltfläche *Einstellungen*, um Ihre persönliche Tracking-Schutz-Liste einzusehen.
In der Adressleiste können Sie durch Klicken auf die Schaltfläche  erkennen, ob neben einer ActiveX-Filterung auch der Tracking-Schutz aktiv ist.

7.7 Privatsphäre schützen mit den InPrivate-Funktionen




Surfen, ohne Spuren auf dem Rechner zu hinterlassen

Möchten Sie verhindern, dass andere Nutzer Ihres Computers nachvollziehen können, welche Webseiten Sie aufgerufen haben, aktivieren Sie die Funktion *InPrivate-Browsen*.

- ✓ Der Internet Explorer öffnet hierdurch ein neues Browserfenster, in dem Sie surfen können, ohne Spuren auf Ihrem Rechner zu hinterlassen.
- ✓ Wenn Sie das Fenster schließen, wird die Funktion *InPrivate-Browsen* wieder deaktiviert. Alle temporären Internetdateien sowie sämtliche angenommenen Cookies werden nach dem Schließen des Fensters automatisch gelöscht.

Während Sie die Funktion *InPrivate-Browsen* nutzen, werden standardmäßig alle selbst installierten Add-Ons deaktiviert.

Die Funktion *InPrivate-Browsen* aktivieren

- ▶ Klicken Sie neben der Adressleiste auf , wählen Sie *Sicherheit* und klicken Sie auf *InPrivate-Browsen*.
- oder Klicken Sie mit der rechten Maustaste in der Taskleiste auf  und dann auf *InPrivate-Browsen starten*.
- ✓ Ein neues Fenster wird geöffnet, das Sie mithilfe der in der Adressleiste angezeigten Meldung  auf die aktivierte Funktion *InPrivate-Browsen* hinweist.
- ✓ Beachten Sie, dass der Schutz Ihrer Privatsphäre beim Surfen nur gewährleistet ist, solange Sie Webseiten in diesem speziellen Fenster aufrufen.


! Die Funktion *InPrivate-Browsen* bewirkt **nicht**, dass Sie **anonym** im Internet surfen können. Bei Nutzung des Internets weist Ihr Provider Ihrem Rechner immer eine eindeutige IP-Adresse zu und speichert eine Liste mit den von Ihnen aufgerufenen Seiten. So lässt sich Ihr Surfverhalten (beispielsweise von hierzu autorisierten Ermittlungsbehörden) auch bei aktivierter Funktion *InPrivate-Browsen* nachvollziehen. Möchten Sie anonym im Internet surfen, nutzen Sie einen sogenannten VPN oder das TOR-Netzwerk – beide verschleiern Ihre IP.

7.8 Automatisches Speichern

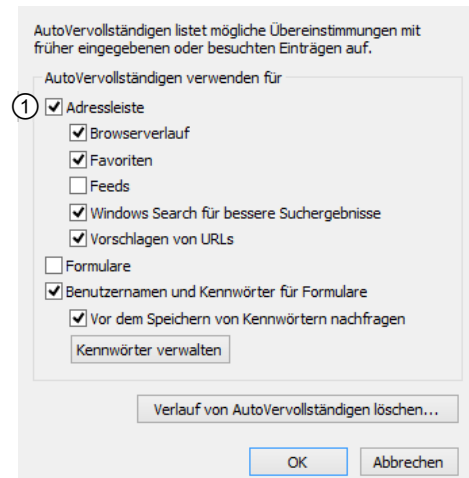
Die AutoVervollständigung nutzen

Ist die AutoVervollständigung aktiviert, werden u. a. der Browserverlauf, die Favoriten sowie Benutzernamen und Kennwörter für Formulare nach der ersten Eingabe gespeichert. Bei erneuter Verwendung werden diese Angaben automatisch aufgerufen.

Automatisches Speichern deaktivieren und den Verlauf löschen


- ▶ Klicken Sie auf  und wählen Sie *Internetoptionen*.
- ▶ Klicken Sie im Fenster *Internetoptionen*, Register *Inhalte*, Bereich *AutoVervollständigungen*, auf *Einstellungen*.
- ▶ Deaktivieren Sie das Kontrollfeld ①, um die Auto-Vervollständigung in der Adressleiste abzuschalten.
oder Deaktivieren Sie alle entsprechenden Kontrollfelder.
- ▶ Klicken Sie abschließend auf *OK*.

Um die Autovervollständigung zu aktivieren, klicken Sie auf die entsprechenden Kontrollfelder und bestätigen mit einem Klick auf *OK*.



7.9 Übung

Sicher im Internet arbeiten

Level		Zeit	ca. 15 min
Übungsinhalte	✓	Sicherheitseinstellungen für den Internet Explorer 10 und Internet Explorer 11	
Übungsdatei	--		
Ergebnisdatei	--		

1. Öffnen Sie den Internet Explorer.
2. Überprüfen Sie auf der Webseite *www.amazon.de* das Sicherheitszertifikat.
3. Ordnen Sie den Webauftritt *www.herdt.com* der Sicherheitszone *Vertrauenswürdige Sites* zu und deaktivieren Sie die Serverüberprüfung auf *https*.
4. Wählen Sie die Website *www.herdt.com* erneut an und aktivieren Sie wieder das Kontrollfeld *Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich*.
5. Löschen Sie alle temporären Internetdateien und deaktivieren Sie im Vorfeld das Beibehalten bevorzugter Websitedaten.
6. Aktivieren Sie die Filterung von ActiveX-Steuerelementen.
7. Aktivieren Sie den Tracking-Schutz.
8. Fügen Sie alle verfügbaren Listen zum Tracking-Schutz hinzu.
9. Aktivieren Sie im Tracking-Schutz die personalisierte Liste.
10. Aktivieren Sie die Funktion *InPrivate-Browsen*.
11. Nehmen Sie alle für diese Übung vorgenommenen Einstellungen zurück.

8

Umgangsformen und Sicherheit im Internet

8.1 Kinderschutz im Internet

Die gezielte Internetnutzung vermitteln und kontrollieren

Der richtige Umgang mit dem Internet ist für Kinder eine zu erlernende Grundfertigkeit – er stellt eine neue Kulturtechnik dar. Der beste Schutz für Kinder ist es, sie anzuleiten, wie sie mit dem Angebot im Internet bewusst und verantwortungsvoll umgehen.

- ✓ Führen Sie Ihr Kind in die Nutzung des Internets ein und bieten Sie ihm Unterstützung an.
- ✓ Ihr Kind sollte zunächst nur gemeinsam mit Ihnen im Internet surfen. So können Sie es direkt auf mögliche Gefahrenquellen aufmerksam machen und diese erklären.
- ✓ Vereinbaren Sie mit Ihrem Kind, dass Angebote aus dem Internet wie Meinungsumfragen oder Gewinnspiele nur nach Absprache mit Ihnen wahrzunehmen sind.
- ✓ Erklären Sie Ihrem Kind, dass es keine persönlichen Daten im Internet bekannt geben soll (beispielsweise Familiennamen, Adresse und Telefonnummer).
- ✓ Stellen Sie kindgerecht aufgebaute Webseiten vor, wie die Seite des Kinderkanals der öffentlich-rechtlichen Sender www.kika.de bzw. www.kikaninchen.de.
- ✓ Stellen Sie Ihrem Kind kindgerechte Suchmaschinen vor, z. B. www.blindekuh.de.
- ✓ Zeigen Sie Ihrem Kind, wie es sein eigenes Profil in einem Social Network wie Facebook privat stellt.
- ✓ Vereinbaren Sie mit Ihrem Kind eine Zeitbeschränkung für die Internetnutzung.

Um das Surfen im Internet oder den Download von Dateien für Kinder zu beschränken bzw. diese zu überwachen, können Sie spezielle Software einsetzen. Diese Software verweigert den Zugriff auf kinder- und jugendgefährdende Inhalte. Weitere Informationen dazu erhalten Sie unter www.computerbild.de/downloads/sicherheit/kindersicherung-internet-509. Alternativ haben Sie auch die Möglichkeit, entsprechende Einstellungen in Ihrem Browser, DSL-Router oder in Ihrer Internet-Security vorzunehmen.

Weitere Tipps für Eltern und Kinder finden Sie beispielsweise auf den folgenden Webseiten:

- ✓ www.saferinternet.at
- ✓ www.bupp.at
- ✓ www.klicksafe.de

Auf Gefahren aufmerksam machen

Die Nutzung verschiedenster Plattformen, sogenannter sozialer Netzwerke wie Facebook oder StudiVZ, gehört für viele genauso zum persönlichen Alltagsleben wie das Pflegen von Kontakten. Leichtsinnig melden sich viele dort unter dem realen Namen an und hinterlassen neben der E-Mail-Adresse und der Telefonnummer weitere ganz persönliche Informationen wie z. B. den Familiennamen und die private Adresse. Die Offenlegung personenbezogener Daten und privater Informationen lädt (IT-)Kriminelle zu betrügerischem Handeln geradezu ein. Betrüger nutzen die Vertrauensseligkeit von Nutzern sozialer Netze aus, um diese z. B. gezielt mit Werbung zu bombardieren. Schadprogramme wie Würmer werden verbreitet und Diebstähle vorbereitet. Auch werden durch Internet-Mobbing bzw. Cyber-Bullying andere Benutzer erniedrigt und boshaft falsche Behauptungen verbreitet. Eine weitere und weitaus größere Gefahr stellt das Grooming dar. Grooming bedeutet in diesem Zusammenhang das gezielte Ansprechen von Kindern und Jugendlichen, mit dem Ziel der Anbahnung sexueller Kontakte. Dabei wird das Vertrauen von jungen Menschen ausgenutzt, um letztendlich pornografische Aufnahmen von ihnen zu machen oder sexuellen Missbrauch an Minderjährigen zu begehen, was einen Straftatbestand darstellt.

Aber auch Arbeitgeber, Vermieter oder Versicherungen nutzen preisgegebene Informationen zu ihrem Vorteil. Diese Informationen können gespeichert werden und tauchen auf anderen Webseiten wieder auf oder sie werden für andere Zwecke genutzt.

Weitere Informationen zum Thema Internet-Mobbing bzw. Cyber-Bullying erhalten Sie auf www.klicksafe.de unter der Rubrik *Themen* im Bereich *Kommunizieren* unter dem Stichwort *Cyber-Mobbing*. Möchten Sie mehr zum Themenfeld „Sicherheit im Internet“ erfahren, finden Sie solche Informationen auf der gleichen Webseite unter der Rubrik *Über Klicksafe* im Bereich *Safer Internet Day*.

8.2 Facebook sicher und richtig nutzen

Legen Sie sich im Vorfeld jeglicher Registrierungen auf sozialen Netzwerken, Chatrooms oder Foren einen zusätzlichen Mail-Account mit fiktiven Daten an. Auf diese Weise ersparen Sie sich einerseits lästige Werbung, andererseits können Sie so besser private Mails von der restlichen E-Mail-Flut trennen. Außerdem hat so nicht jeder Benutzer die Möglichkeit, Sie via Mail zu kontaktieren.

Facebook dient im Folgenden als praktisches Beispiel für die Registrierung und Nutzung von sozialen Netzwerken. Ein Großteil der hier genannten Einstellungen kann auf diverse Netzwerke übertragen werden.



Viele Webseiten bieten mit dem Facebook-Button *gefällt mir* die Möglichkeit, die besuchte Seite mit dem eigenen Profil zu verbinden und somit stets auf dem aktuellen Stand zu bleiben. Aus datenschutztechnischer Sicht ist dieser Button als problematisch anzusehen, da durch den Besuch einer Webseite mit entsprechendem Button, egal ob ein Facebook-Account eingerichtet oder der Benutzer auf Facebook eingeloggt ist, die IP-Adresse an Facebook übermittelt wird. Die damit verbundene Datenerhebung sowie das Ablegen eines Cookies auf dem PC kann bei dem Internetbrowser **Firefox** durch die Installation sogenannter Add-ons, wie z. B. **Disconnect**, **NoScript**, **Ghostery** und **Adblock Edge**, unterbunden werden. Nebenbei werden durch die Add-ons auch Werbung und Cookies anderer Anbieter auf allen Webseiten blockiert.

8.3 Privatsphäre und Standort bei Facebook einrichten

In der Standardeinstellung sind zunächst alle Informationen öffentlich einsehbar. Alle Aktionen, die Sie auf Facebook ausführen, werden in Ihrer Chronik dokumentiert. Befinden sich darin sehr viele Informationen, Nachrichten, Bilder usw., wählt Facebook zur Vereinfachung der Darstellung Daten aus, die für Sie von besonderer Bedeutung sein könnten. Je weiter die Ereignisse in der Vergangenheit liegen, desto weniger Angaben werden angezeigt. Diese automatische Auswahl und Veröffentlichung Ihrer Daten entspricht meistens nicht den eigenen Wünschen. Sie können jedoch über individuelle und allgemeine Einstellungen selbst festlegen, was sich in Ihrer Chronik befindet bzw. wer diese Informationen sehen darf.



Um zu vermeiden, dass jeder Facebook-Benutzer Ihre Daten und Ihren Standort sehen oder auch Facebook diese Daten gezielt für Werbung nutzen kann, stehen Ihnen verschiedene Möglichkeiten zur Verfügung:

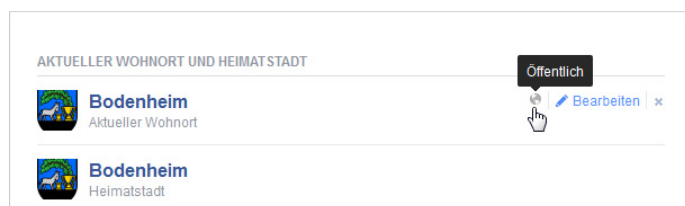
- ✓ Speichern Sie nicht zu viele Angaben über Ihre Person.
- ✓ Legen Sie fest, welche Facebook-Benutzergruppe mit welchen Rechten Einblick in Ihre Inhalte erhält.
- ✓ Nehmen Sie entsprechende Einstellungen im Bereich der Privatsphäre vor.

Einstellungen zur Privatsphäre und zum Standort vornehmen

Die Einstellungen zur Privatsphäre und zum Standort sollten Sie schon bei der Eingabe von Informationen festlegen bzw. prüfen. Sie können jedoch auch nachträglich entsprechende Einstellungen vornehmen. Vermeiden Sie jedoch im Vorfeld die Eingabe zu vieler persönlicher Daten, damit diese später nicht einzeln wieder eingeschränkt oder gelöscht werden müssen.

Privatsphäre- und Standort-Einstellungen für Profilangaben vornehmen

- ▶ Klicken Sie in der Chronik auf *Info*.
- ▶ Wählen Sie auf der Infoseite eine Kategorie, z. B. *Orte, an denen du gelebt hast* und klicken Sie im rechten Bereich neben einem Eintrag auf .
- ▶ Klicken Sie auf  Öffentlich und wählen Sie aus, welche Benutzergruppe diese Information einsehen darf z. B. *Freunde* oder *Nur Ich*, wenn keiner diese Informationen sehen soll.
- ▶ Klicken Sie auf *Änderungen speichern*.
Nur die Benutzer, die Sie bei Facebook als Freunde hinzugefügt haben, können nun die betreffenden Informationen (z. B. Ihren Wohnort) sehen.



Standort-Einstellungen in Profilangaben bearbeiten und entfernen

Um Standortdaten aus Ihrem Facebook-Profil zu entfernen, gehen Sie wie folgt vor.

- ▶ Klicken Sie in der Chronik auf *Info*
- ▶ Wählen Sie auf der Infoseite eine Kategorie, z. B. *Orte, an denen du gelebt hast* und klicken Sie im rechten Bereich neben einem Eintrag z. B. *Aktueller Standort* auf *Bearbeiten*.

The screenshot shows the 'AKTUELLER WOHNORT UND HEIMATSTADT' section of a Facebook profile. The 'Aktueller Wohnort' is set to 'Bodenheim'. A 'Heimatsstadt' field is also present. A dropdown menu is open for the 'Aktueller Wohnort' entry, showing options: 'Öffentlich' (selected), 'Freunde', 'Nur ich', 'Benutzerdefiniert', 'Enge Freunde', and 'Alle Listen anzeigen ...'. The 'Änderungen speichern' button is visible. Three numbered callouts are present: 1. 'Hier den Eintrag entfernen' points to the 'Aktueller Wohnort' entry. 2. 'Hier klicken und Nur ich auswählen' points to the 'Nur ich' option in the dropdown menu. 3. 'Auf Änderungen speichern klicken' points to the 'Änderungen speichern' button.

Privatsphäre- und Standort-Einstellungen für Statusmeldungen vornehmen

Die Privatsphäre-Einstellungen stehen Ihnen auch beim Hinzufügen von Statusmeldungen, Fotos, Orten und Lebensereignissen zur Verfügung. Mit einer Statusmeldung können Sie einer interessierten Benutzergruppe etwas unverbindlich mitteilen. Beim Versenden einer Nachricht wenden Sie sich dagegen gezielt an einen oder mehrere Adressaten.

Die aktiven Einstellungen erkennen Sie schnell an den Symbolen (*Öffentlich*), (*Freunde*), (*Nur ich*), (*Benutzerdefiniert*).

- ▶ Klicken Sie auf das Feld unterhalb Ihres Profilbildes.
- ▶ Geben Sie eine Statusmeldung ein.
- ▶ Klicken Sie auf *Öffentlich* () und wählen Sie eine Gruppe von Nutzern aus, die Ihre Nachricht bei Interesse lesen darf (z. B. *Freunde*).
- ▶ Klicken Sie auf *Posten*, um die Meldung zu verschicken.

The screenshot shows the Facebook status creation interface. The status text is 'Ich fliege gerade der Abendsonne entgegen!'. Below the text are icons for adding photos, tags, emojis, locations, and a clock. The privacy dropdown is set to 'Öffentlich'. A dropdown menu is open showing the 'Wer soll das sehen?' options: 'Öffentlich' (selected), 'Freunde', and 'Weitere Optionen'. The 'Freunde' option is highlighted.

Standort-Einstellungen in Statusmeldungen entfernen

Möchten Sie eventuelle Standortdaten in neuen Statusmeldungen entfernen, gehen Sie wie folgt vor.



Daten in der Chronik löschen


Sie können Inhalte in der Chronik (z. B. Statusmeldungen, Fotos etc.) jederzeit löschen. Dies gilt auch für Inhalte, die Sie den Chroniken anderer Personen hinzugefügt haben.

- ▶ Zeigen Sie auf den Inhalt (bzw. ein Foto, Video etc.).
- ▶ Klicken Sie im rechten oberen Eck auf ▼ und wählen Sie *Löschen*.
- ▶ Bestätigen Sie die Rückfrage mit *Beitrag löschen*.



Standardeinstellungen für die Privatsphäre

Sofern Sie keine individuellen Einstellungen für die Privatsphäre vorgenommen haben, sind standardmäßig alle Informationen zu Ihrer Person öffentlich zugänglich. Um nicht bei jeder Texteingabe die Privatsphäre festlegen zu müssen, können Sie die Standardeinstellungen selbst festlegen und gleichzeitig Ihre Privatsphäre schützen.

- ▶ Klicken Sie in Ihrem Facebook-Account auf .
- ▶ Klicken Sie in der eingeblendeten Liste nacheinander auf die Einträge, beginnend z. B. mit *Wer kann meine Inhalte sehen?*.
- ▶ Klicken Sie auf die eingeblendete Schaltfläche, z. B. *Freunde*, und dann auf *Weitere Optionen* und auf *Benutzerdefiniert*, wenn Sie individuelle Privatsphäre-Einstellungen vornehmen möchten.

Alternativ zur Option *Benutzerdefiniert* können Sie auch eine der vorgegebenen Optionen, z. B. *Freunde*, auswählen.



- ▶ Wählen Sie unter *Das mit folgenden Personen teilen* im Feld *Diese Personen oder Listen* eine der folgenden Optionen aus.

Klicken Sie auf ...

- ✓ *Freunde von Freunden*, um für alle Freunde und deren Freunde Ihre Inhalte einsehbar zu machen.
- ✓ *Freunde*, um für alle Freunde Ihre Inhalte einsehbar zu machen.

Im Bereich *Nicht teilen mit* können Sie im Feld *Diese Personen oder Listen* bei Bedarf Personen/Listen vom Zugriff auf Ihre Inhalte ausschließen.

Unabhängig von Ihrer gewählten Standardeinstellung können Sie weiterhin die Privatsphäre eines Beitrags individuell über die Symbole (*Öffentlich*), (*Freunde*), (*Nur ich*), (*Benutzerdefiniert*) und (*Enge Freunde*) einstellen.

8.4 Anwendungen und Inhalte einschränken

Chronik und Markierungen

Über diese Einstellungen können Sie bestimmen, ob ein anderer Benutzer in Ihrer Chronik Einträge hinzufügen oder Sie auf einem Foto oder in einer Nachricht eindeutig identifizieren darf.

Das Markieren von Personen auf unvorteilhaften Fotos kann verletzend oder erniedrigend wirken und dadurch die Privatsphäre empfindlich stören.

- ▶ Klicken Sie auf und wählen Sie *Einstellungen*.
- ▶ Klicken Sie im Navigationsbereich auf *Chronik und Markierungen*.
- ▶ Klicken Sie in den verschiedenen Bereichen auf einen Link, z. B. *Bearbeiten*, und nehmen Sie die gewünschten Einstellungen vor.

Chronik und Markierungseinstellungen

Wer kann Inhalte zu meiner Chronik hinzufügen?	Wer kann in deiner Chronik posten?	Nur ich	Bearbeiten
	Möchtest du die Beiträge überprüfen, in denen du von Freunden markiert wurdest, bevor sie in deiner Chronik erscheinen?	Ein	Bearbeiten

Werbeanzeigen, Anwendungen und Webseiten

Ein nicht unerhebliches Risiko für Ihre Privatsphäre entsteht bei der Nutzung von Anwendungen (sogenannten Apps) innerhalb von Facebook. Um diese Sicherheitslücke zu schließen, können Sie von vornherein diese Anwendungen von der Benutzung ausschließen.

- ▶ Klicken Sie im Navigationsbereich auf *Werbeanzeigen* und in den verschiedenen Bereichen auf einen Link, z. B. *Bearbeiten*, und nehmen Sie die gewünschten Einstellungen vor.

Facebook-Werbeanzeigen

Webseiten Dritter

Facebook berechtigt Anwendungen Dritter bzw. Werbenetzwerke weder zur Nutzung deines Namens noch zur Nutzung deines Bildes für Werbeanzeigen. Sollten wir dies in Zukunft gestatten, so wird die von dir ausgewählte Einstellung die Nutzung deiner Informationen regeln.


Du kannst durch soziale Plug-ins von Facebook soziale Kontexte auf Webseiten Dritter, unter anderem in Werbeanzeigen, sehen. Obwohl dir soziale Plug-ins eine soziale Nutzererfahrung auf Webseiten Dritter ermöglichen, teilt Facebook deine Informationen nicht mit den Webseiten der Drittparteien, auf welchen sich die sozialen Plug-ins befinden. Erfahre mehr über [soziale Plug-ins](#).

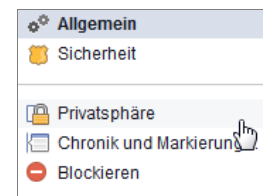
 [Bearbeiten](#)

- ▶ Klicken Sie zum Speichern der Änderung auf *Änderung speichern*.
- ▶ Klicken Sie im Navigationsbereich auf *Apps*, um die Berechtigungen von Apps auf Facebook einzuschränken.

Beschränken Sie das Publikum für ältere Beiträge

Beiträge, die Sie in der Vergangenheit geschrieben und nicht ausreichend geschützt haben, können Sie nachträglich nur für Freunde sichtbar machen.

- ▶ Klicken Sie auf  und wählen Sie *Einstellungen*.
- ▶ Klicken Sie im Navigationsbereich auf *Privatsphäre*.
- ▶ Klicken Sie unter *Wer kann meine Inhalte sehen?* auf den Link *Vergangene Beiträge einschränken* und betätigen Sie *Alte Beiträge beschränken*.
- ▶ Speichern Sie die vorgenommene Einstellung durch Klicken auf *Bestätigen* und *Schließen*.



Privatsphäre-Einstellungen und Werkzeuge

Wer kann meine Inhalte sehen?

Wer kann deine zukünftigen Beiträge sehen?

Freunde

[Bearbeiten](#)

Überprüfe alle deine Beiträge und Inhalte, in denen du markiert bist


[Aktivitätenprotokoll verwenden](#)

Möchtest du die Zielgruppe für Beiträge einschränken, die du mit Freunden von Freunden oder öffentlich geteilt hast?

 [Vergangene Beiträge einschränken](#)

Blockierte Personen und Anwendungen

Möchten Sie Nutzer blockieren, sodass diese nicht mehr auf Facebook mit Ihnen in Kontakt treten können, gehen Sie wie folgt vor:

- ▶ Klicken Sie auf  und wählen Sie *Einstellungen*.
- ▶ Klicken Sie im Navigationsbereich auf *Blockieren* und tragen Sie unter *Nutzer blockieren* im Feld *Name oder E-Mail hinzufügen* den Namen oder die E-Mail-Adresse des Benutzers ein, der blockiert werden soll.
- ▶ Klicken Sie jeweils auf *Blockieren*.
Anschließend erscheint der Name bzw. die E-Mail-Adresse, die zukünftig blockiert wird.

Wissen Sie etwas über eine missbräuchliche Nutzung sozialer Netzwerke, können Sie dies dem Service-Provider, der Polizei oder beispielsweise auch dem Bundesamt für Informationstechnik melden.

9

Sicher kommunizieren und mobil arbeiten

9.1 E-Mails signieren und verschlüsseln

Sicherheitszertifikate einsetzen

Beim Verschicken von Briefen oder Faxen können Sie mit Ihrer Unterschrift sicherstellen, dass Sie tatsächlich der Urheber des Schriftstückes sind. Um eine vergleichbare Sicherheit im E-Mail-Verkehr herzustellen, versenden Sie Ihre Nachrichten mit einer digitalen ID (Zertifikat).

- ✓ Zertifikate dienen dem Unterzeichnen von E-Mails. So kann der Empfänger sicher sein, dass die E-Mail nicht gefälscht wurde.
- ✓ Mit bestimmten Zertifikaten können E-Mails auch verschlüsselt werden. Verschlüsselte E-Mails können nur von jenen Empfängern entschlüsselt und gelesen werden, die auch ein Zertifikat besitzen.
- ✓ Zertifikate können eingesetzt werden, um die eigene Identität bei der Übermittlung elektronischer Daten nachzuweisen, beispielsweise beim Onlinebanking: Hier muss gewährleistet sein, dass Sie tatsächlich der Kontoinhaber sind.
- ✓ Webseiten-Zertifikate bescheinigen, dass die Webseite authentisch und echt ist. Dies ist beispielsweise bei Webseiten wichtig, bei denen Sie persönliche Daten wie Benutzername, Kennwort, Bankverbindung und ähnliche Daten angeben können.

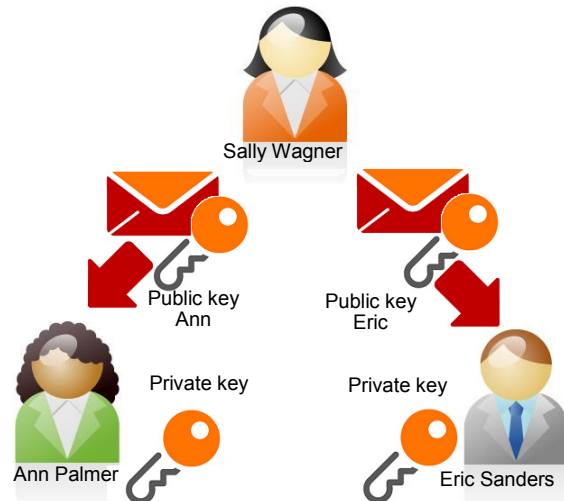
Sicherheitszertifikate und Nachrichtenverschlüsselung

Ein persönliches Zertifikat besteht aus drei Komponenten: einer digitalen Signatur zum Unterzeichnen von E-Mails sowie einem öffentlichen und einem privaten Schlüssel zum Verschlüsseln von E-Mails. Die digitale Signatur ist eine kryptische Folge von Zeichen, die aus dem Inhalt des Dokuments mithilfe des privaten Schlüssels berechnet wird und als elektronische Unterschrift dem Dokument hinzugefügt wird. Mithilfe des öffentlichen Schlüssels kann der Nachrichtempfänger prüfen, ob das Dokument und die Unterschrift zusammenpassen, d. h. nicht gefälscht sind. Das Verschlüsseln der Daten mithilfe eines öffentlichen und eines privaten Schlüssels wird auch als **Public-Key-Algorithmus** bezeichnet.

Der öffentliche Schlüssel (**Public Key**) ist frei verfügbar und unterliegt keiner Geheimhaltung. Der private Schlüssel ist geheim und benutzerspezifisch (**Private Key**) und muss unter Verschluss gehalten werden.

Nur mithilfe des privaten Schlüssels aus einem Schlüsselpaar kann die E-Mail entschlüsselt werden.

- ✓ Um z. B. an Eric Sanders und Ann Palmer verschlüsselte Nachrichten schicken zu können, muss Sally Wagner jeweils den öffentlichen Schlüssel von Eric Sanders und Ann Palmer besitzen.
- ✓ Eric Sanders und Ann Palmer können nun mit ihrem jeweiligen privaten Schlüssel die Nachricht entschlüsseln.



Funktionsweise des Public-Key-Algorithmus

Persönliches Zertifikat (digitale ID) anfordern

Sicherheitszertifikate werden von unabhängigen Zertifizierungsstellen (Trust Center) ausgestellt. Sie können ein persönliches Zertifikat anfordern, indem Sie sich auf die Webseite eines Zertifikatsausstellers begeben und dort Ihre persönlichen Daten eingeben. Die Gültigkeit der Sicherheitszertifikate wird von Zertifizierungsstellen überwacht. Die meisten Sicherheitszertifikate besitzen ein Ablaufdatum.

Neben weiteren Unternehmen bietet die Firma Verisign kostenpflichtige digitale IDs an. Diese haben eine Gültigkeit von einem Jahr und können über die Webseite www.verisign.com/authentication/digital-id/index.html?tid=gnps bezogen werden. Ähnlich den digitalen IDs, soll die De-Mail einen gesicherten und authentifizierten Mailverkehr zulassen.

Zertifikat erstellen

Verschiedene Provider bieten auch die Möglichkeit, entsprechende Zertifikatsdateien zu erstellen und herunterzuladen.

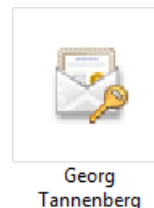
Als Beispiel ist die Erstellung beim Free-mailer *Web.de* aufgezeigt.

- ▶ Geben Sie ein Kennwort ein ① und bestätigen Sie Ihre Eingabe ② noch einmal.
- ▶ Klicken Sie anschließend auf die Schaltfläche ③, um das digitale Zertifikat herunterzuladen.

Gültig von 17.04.2014 bis 17.04.2017	
Fingerprint: [blurred]	
Public Key:	
-----BEGIN PUBLIC KEY----- [blurred] -----END PUBLIC KEY-----	
So verwenden Sie Ihr Zertifikat in einem E-Mail-Programm:	
1. Schritt: Legen Sie ein Kennwort für den privaten Schlüssel fest.	
Kennwort:	[blurred] ①
Kennwort wiederholen:	[blurred] ②
2. Schritt: Speichern Sie das Zertifikat auf Ihrem Computer.	
Zertifikat exportieren ③	

Privaten Schlüssel auf den Rechner installieren

- ▶ Klicken Sie doppelt auf das Zertifikat.
Es wird ein Assistent geöffnet, der das Zertifikat in den verschiedenen Anwendungen installiert.
- ▶ Wählen Sie einen Speicherort aus und klicken Sie auf *Weiter*.
- ▶ Bestätigen Sie die eingetragene Datei mit *Weiter* oder klicken Sie auf *Durchsuchen*, um ein anderes Zertifikat zu wählen.
- ▶ Geben Sie das Passwort ein ①, um die Gültigkeit zu bestätigen.
- ▶ Aktivieren Sie gegebenenfalls das Kontrollfeld ②, um die hohe Sicherheitsstufe zu aktivieren.
- ▶ Einen privaten Schlüssel vom Typ PKCS #12 (.p12) können Sie exportieren, wenn Sie das Kontrollfeld ③ aktivieren.
- ▶ Bestätigen Sie Ihre Einstellungen mit *Weiter*, klicken Sie auch im folgenden Fenster auf *Weiter* und schließen Sie die Installation im letzten Fenster durch *Fertig stellen* ab.
- ▶ Bestätigen Sie den erfolgreichen Importvorgang im eingeblendeten Hinweis mit *OK*.



Schutz für den privaten Schlüssel
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort: ①

☐ Kennwort anzeigen

Importoptionen:

② ☐ Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.

③ ☐ Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.

☒ Alle erweiterten Eigenschaften mit einbeziehen

Weitere Informationen über das [Sichern privater Schlüssel](#)

Outlook zur Verwendung mit dem Zertifikat konfigurieren

- ▶ Klicken Sie im Register *Datei* auf *Optionen*.
- ▶ Klicken Sie auf die Kategorie *Sicherheitscenter* bzw. *Trust Center* und dort auf *Einstellungen für das Sicherheitscenter* bzw. auf *Einstellungen für das Trust Center*.
- ▶ Klicken Sie in der Kategorie *E-Mail-Sicherheit* auf *Einstellungen*.
- ▶ Überschreiben Sie gegebenenfalls im Fenster *Sicherheitseinstellungen ändern* den Namen ① für diese Sicherheitseinstellung.
- ▶ Klicken Sie auf die Schaltfläche ② und wählen Sie im geöffneten Fenster das gewünschte Zertifikat aus.
- ▶ Schließen Sie das Fenster mit *OK*.
Standardmäßig wird das ausgewählte Zertifikat auch als Verschlüsselungszertifikat eingetragen ③.
- ▶ Schließen Sie die Fenster mit *OK*.

Bevorzugte Sicherheitseinstellungen

Name der Sicherheitseinstellung: ①

Kryptografieformat:

☐ Standardeinstellung für dieses Format kryptografischer Nachrichten

☐ Standardsicherheitseinstellung für alle kryptografischen Nachrichten

Zertifikate und Algorithmen

Signaturzertifikat: ②

Hashalgorithmus:

Verschlüsselungszertifikat: ③

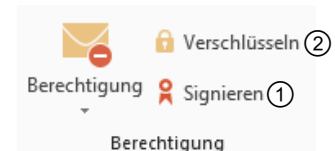
Verschlüsselungsalgorithmus:

☒ Signierten Nachrichten diese Zertifikate hinzufügen

Persönliches Zertifikat an einen Empfänger schicken

Bevor Sie einem Empfänger verschlüsselte Nachrichten senden können, müssen Sie ihm eine Nachricht mit Ihrer digitalen Signatur zukommen lassen. Sie können, unabhängig von Ihren vorgewählten Einstellungen, für jede ausgehende Nachricht einzeln entscheiden, welche Sicherheitseinstellungen Sie verwenden möchten.

- ▶ Erstellen Sie eine neue Nachricht. Aktivieren Sie im Nachrichtenformular im Register *Optionen*, Gruppe *Berechtigung*, die Schaltfläche ①.
- ▶ Wenn die Nachricht zusätzlich verschlüsselt werden soll, aktivieren Sie in der Gruppe *Berechtigung* die Schaltfläche ②.
- ▶ Versenden Sie die Nachricht.



Je nach den gewählten Sicherheitseinstellungen (hoch bzw. mittel) werden Sie im nun eingeblendeten Fenster aufgefordert, den Zugriff auf Ihren privaten Schlüssel zu bestätigen (Option *Berechtigung erteilen*) bzw. das Kennwort einzugeben.

Alle Nachrichten digital signieren und/oder verschlüsseln

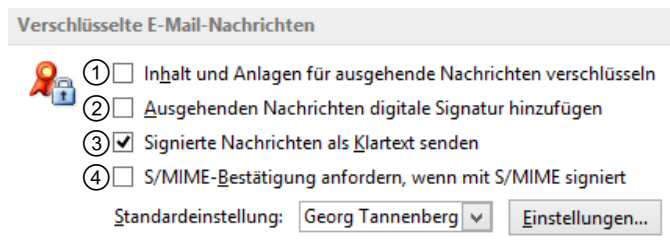
Wenn Sie häufig eine digitale Signatur bzw. eine Verschlüsselung ausgehender Nachrichten benötigen, können Sie diese Einstellungen im Fenster *Outlook-Optionen* in der Kategorie *Sicherheitscenter* vorwählen.

- ▶ Klicken Sie im Register *Datei* auf *Optionen*.
- ▶ Klicken Sie im Fenster *Outlook-Optionen* in der Kategorie *Sicherheitscenter* bzw. *Trust Center* auf *Einstellungen für das Sicherheitscenter* bzw. auf *Einstellungen für das Trust Center*.
- ▶ Wechseln Sie in die Kategorie *E-Mail-Sicherheit*.

①, ② Alle ausgehenden Nachrichten werden signiert bzw. verschlüsselt.

③ Empfänger, deren E-Mail-Programm die digitale Signatur nicht überprüfen kann, können Ihre E-Mails dennoch im Klartext lesen.

④ Ihre signierten E-Mails können von den Empfängern nicht im Vorschaufenster gelesen werden.



- ▶ Beenden Sie den Vorgang mit einem Klick auf *OK*.

Persönliches Zertifikat eines Empfängers im Ordner *Kontakte* aufnehmen

Um einer bestimmten Person eine verschlüsselte E-Mail senden zu können, benötigen Sie neben Ihrem eigenen persönlichen Zertifikat auch eine digital signierte E-Mail von dieser Person. Fügen Sie die digitale ID dieser Person deren Kontaktformular in Ihrem Ordner *Kontakte* hinzu. Dadurch speichern Sie den öffentlichen Schlüssel dieser Person auf Ihrem Rechner.

- ▶ Öffnen Sie die empfangene Nachricht mit der digitalen ID.
- ▶ Klicken Sie mit der rechten Maustaste auf den Absender.
- ▶ Wählen Sie den Kontextmenüpunkt *Zu Outlook-Kontakten hinzufügen*.
Das Kontaktformular wird geöffnet.
- ▶ Klicken Sie im Register *Kontakt*, Gruppe *Anzeigen*, auf die Schaltfläche *Zertifikate*, um die digitale ID des Absenders angezeigt zu bekommen.
- ▶ Klicken Sie auf die Schaltfläche *Speichern und Schließen*, um das Kontaktformular zu schließen.
Falls der Kontakt bereits existiert, wird das Fenster *Mehrfach vorhandener Kontakt* geöffnet.
- ▶ Bestätigen Sie die standardmäßig ausgewählte Option zum Aktualisieren des Kontaktes.

Sie können nun verschlüsselte Nachrichten an diesen Kontakt senden. Die Verschlüsselung erfolgt über den öffentlichen Schlüssel, den Sie von diesem Kontakt besitzen. Das Entschlüsseln erfolgt beim Empfänger mit dessen privatem Schlüssel.

9.2 Kommunikation mit VoIP und Instant Messaging

Unter VoIP (Voice over Internet Protocol) bzw. IP-Telefonie versteht man das Telefonieren über das Internet. So können zur Kommunikation dank spezieller Apps Smartphones, Tablets und PCs aber auch geeignete IP-Telefone oder aber auch klassische Telefone, die über spezielle Adapter verfügen, genutzt werden. Ähnlich wie bei VoIP nutzt IM (Instant Messaging oder Nachrichten-sofortversand) zur Übertragung das Internet. Bei dieser Kommunikationsmethode unterhalten sich die Teilnehmer per Textnachrichten (ähnlich der SMS).

Da sowohl VoIP als auch IM Daten und Informationen über das Internet übertragen, sind diese Kommunikationsmethoden besonders anfällig für Malware, Backdoor access und Lauschangriffe. Zur sicheren Kommunikation empfiehlt sich ...

- ✓ die **Nicht-Offenlegung wichtiger Daten** (vermeiden Sie, wichtige Daten unverschlüsselt über unverschlüsselte Kanäle über das Internet zu versenden – Hacker könnten sich diese Daten und Informationen widerrechtlich aneignen);
- ✓ die **Beschränkung der gemeinsamen Dateinutzung** (je weniger Nutzer gemeinsam an Dateien arbeiten, desto geringer ist die Gefahr, dass ungewollt Zugangsdaten in falsche Hände geraten);
- ✓ die **Verschlüsselung jeglicher Kommunikation** (verschlüsseln Sie mithilfe entsprechender Apps z.B. beim Smartphone mit den Apps Signal oder Threema Ihre Kommunikation, um zu vermeiden, dass Dritte Sie abhören).

9.3 Mobile Geräte

App-Store

Um mit mobilen Geräten, wie Smartphones und Tablets produktiv arbeiten zu können, benötigen Sie Apps, wie z.B. die bereits genannten Smartphone-Apps RedPhone, TextSecure und Threema. Wurden Computerprogramme früher in Geschäften gekauft, kauft man heute Apps in App-Stores – diese stellen die gewünschten Apps und eine Bezahlungsfunktion zur Verfügung. Neben den offiziellen App-Stores gibt es auch unzählige inoffizielle App-Stores, bei denen Sie Apps beziehen können. Bei inoffiziellen App-Stores kann es aber durchaus vorkommen, dass Apps Malware enthalten, unnötige viele Ressourcen verbrauchen, personenbezogene Daten an Dritte weiterleiten, versteckte Kosten verursachen oder einfach auch nur von schlechter Qualität sind.

Möchten Sie eine App aus einem App-Store beziehen, müssen Sie diese installieren. Vor einer jeden Installation informiert Sie der App-Store über die Berechtigungen der zu installierenden App. Hierbei wird aufgelistet, welche Anforderungen die App hat und ob sie z.B. auf Ihre Kontakte, Ihre Position, Fotos/Medien/Dateien oder aber auf Ihr Telefon zugreift. So benötigt z.B. eine App zum Instant-Messaging unter anderem Zugriff auf Ihre Kontakte und Dateien, damit Sie mit anderen kommunizieren und Daten austauschen können. Achten Sie aber darauf, dass die Berechtigungen der zu installierenden App logisch sind - eine Taschenlampen-App benötigt keinen Zugriff auf Ihre Position, auf Fotos/Medien/Dateien geschweige denn auf Ihr Telefon. Viele Apps übermitteln zudem auch private Informationen, wie Kontaktdaten, Standortverlauf und Bilder an deren Urheber, die die gesammelten Informationen weiterverwerten oder an Dritte verkaufen.

Geräteverlust

Haben Sie das Smartphone oder das Tablet verloren oder wurde es gestohlen, können Sie dies mit speziellen Apps, die zuvor auf dem Gerät installiert wurden, orten bzw. aus der Ferne löschen oder sperren, so dass Dritte nicht an Ihre persönlichen Daten kommen und je nach App, das Gerät sogar unbrauchbar wird. Um das Gerät ausfindig zu machen, wird mithilfe der Datenverbindung und des GPS (Global Positioning System), ähnlich wie bei der Navigation mit dem Auto, der aktuelle Standort Ihres Geräts bestimmt. Die Datenverbindung zu dem Gerät dient auch dazu, das Gerät zu sperren oder es zu löschen.

10

Datensicherheitsmanagement

10.1 Datensicherung – Backups

Datensicherung für Notfälle

Um ein Gespür für diese Thematik zu entwickeln, stellen Sie sich kurz vor, dass die Festplatte in Ihrem Rechner defekt wäre. Die Inhalte wären damit verloren. Wenn Sie jetzt den Verlust und die Möglichkeiten zur Wiederherstellung betrachten, können Sie zwei Arten von verlorenen Daten unterscheiden:

- ✓ Betriebssystem und installierte Anwendungen lassen sich neu installieren. Das kostet Zeit, die für andere produktive Arbeit verloren geht.
- ✓ Alle Daten, das heißt Dokumente, die Sie erstellt oder bearbeitet haben, sind verloren.

Anhand dieser beiden Faktoren können Sie nun versuchen, den Verlust zu beziffern. Der Aufwand, den Sie für die Datensicherung betreiben, sollte in einem vernünftigen Verhältnis zu diesem Verlust stehen. Um den Aufwand abzuschätzen, müssen Sie die Fragen beantworten:

- ✓ Was bzw. welche Daten sichern?
- ✓ Womit und worauf, das heißt auf welches Medium, sichern?

Was sichern?

Unwiederbringlich verloren sind im Ernstfall alle Dateien, die Sie selbst erstellt bzw. bearbeitet haben. Sie sollten auf jeden Fall gesichert werden. Alles, was installiert wurde, ändert sich normalerweise eher selten und muss dementsprechend auch nicht so oft gesichert werden.

Eine durchdachte Ablagestruktur (wo werden welche Dateien gespeichert?) verringert hierbei den Aufwand immens. Wenn Sie zum Speichern von Daten-Dateien eigene Ordner oder Laufwerke benutzen, ist es einfacher, die relevanten Dateien auszuwählen. In Netzwerken speichern Benutzer solche Dateien üblicherweise auf speziellen Netzlaufwerken. Dies erleichtert die Datensicherung ungemein, da sie nur noch an wenigen zentralen Stellen erfolgen muss.

Wohin sichern?

Ziel sollte immer die Datensicherung auf ein Medium sein, d. h., nach der Sicherung befinden sich die Daten auf einem Datenträger, der physikalisch vom Computer getrennt ist. Außerdem können die Daten an einem sicheren Ort gelagert werden. Es bieten sich unterschiedliche Möglichkeiten an, die mit verschiedenen Vor- und Nachteilen behaftet sind:

Medium	Vorteile	Nachteile
Backup auf derselben Festplatte	Schnell und einfach	Kein Schutz gegen Viren, Anwenderfehler oder Festplattendefekt
Andere Festplatte	Gute und schnelle Lösung, wenn die Festplatte in einem Wechselrahmen steckt oder extern über USB betrieben und nach der Sicherung entfernt werden kann	Teuer, erfordert den Einbau eines Wechselrahmens bzw. einer zusätzlichen Festplatte (extern)
CDs/DVDs/Blu-rays	Preiswert; gut geeignet für den Hausgebrauch	Mittlere Speicherkapazität, ein CD/DVD/Blu-ray-Brenner muss vorhanden sein, Lagerzeit/-ort
Sicherungs-bänder	Professionelles Verfahren mit hohen Kapazitäten und mehrfach verwendbaren Medien zu akzeptablen Preisen; verschiedene Ausführungen für unterschiedlichen Bedarf	Setzt spezielle Hardware (Streamer) voraus, die teuer in der Anschaffung ist
Cloud-Service	Schnell, einfach und überall abrufbar	Cloud-Service kann insolvent werden, Daten können durch Hackerangriffe in falsche Hände geraten

Unabhängig von der Sicherung lokaler Dateien werden die Inhalte firmenweiter Netzlaufwerke in regelmäßigen Abständen auf gesonderte Speichermedien gesichert. Durch das Speichern wichtiger Dokumente im Netzwerk werden diese Daten automatisch gesichert.

Unabhängig davon, welches Medium Sie benutzen, sollten Sie sich auf jeden Fall über die folgenden Themen einige zusätzliche Gedanken machen:

- ✓ **Haltbarkeit:** Wie lange sollen die Daten archiviert werden? Die meisten Hersteller geben hierzu Werte an.
- ✓ **Lagerung:** Die Lagerung kann direkten Einfluss auf die Haltbarkeit haben. Magnetische Aufzeichnungsverfahren wie Festplatten oder Sicherungsbänder reagieren empfindlich auf magnetische Felder. CDs/DVDs/Blu-rays sollten keinen direkten Lichtquellen und höheren Temperaturen ausgesetzt werden.
- ✓ **Komprimierung:** Werden die Daten während der Sicherung komprimiert, benötigen diese weniger Speicher auf dem jeweiligen Speichermedium.
- ✓ Hierzu gehört auch der Sicherheitsaspekt. Die Medien könnten gestohlen oder durch einen Brand vernichtet werden. Ein feuersicherer Safe, am besten in einem anderen Gebäude, bietet hier zusätzlichen Schutz.
- ✓ **Erfolg der Datensicherung:** Zu einer guten Sicherungsstrategie gehören auch regelmäßige Wiederherstellungstests, um sich gegen Aufzeichnungsfehler abzusichern. Eine regelmäßige Datensicherung hilft nicht, wenn Sie im Notfall feststellen, dass Sie auf die vermeintlich gesicherten Daten nicht zugreifen können.

Wie oft sichern?

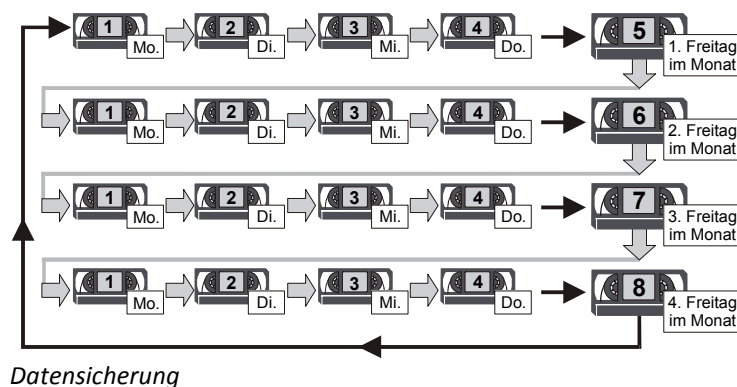
Die Beantwortung dieser Frage hängt stark davon ab, wie häufig sich die Daten ändern und wie hoch Sie den Wert der Daten einschätzen. Für Online-Geschäfte, bei denen Hunderte von Vorgängen jede Stunde anfallen, sind weitaus komplexere Sicherungsstrategien notwendig als an Ihrem PC zu Hause.

Datensicherungsstrategien

Im Folgenden wird beispielhaft eine Datensicherungsstrategie vorgestellt, die u. a. für Schreibbüros üblich ist. Dabei werden alle Daten auf einem zentralen File-Server gespeichert, der mit gesonderten Festplatten ausgestattet ist. Die Daten werden täglich nach einem bestimmten System auf unterschiedliche Festplatten gesichert. Sie sind folgendermaßen beschriftet und werden entsprechend eingesetzt:

Montag, Dienstag, Mittwoch, Donnerstag, Freitag1, Freitag2, Freitag3, Freitag4

Die Freitags-Festplatten werden abwechselnd benutzt. Damit haben Sie eine Sicherung, die den Stand der letzten fünf Tage abdeckt, können im Notfall aber auch drei Wochen zurückspringen. Diese Strategie lässt sich durch das Einführen weiterer Festplatten (Januar, Februar ...; 2015, 2016 ...) beliebig erweitern.



Womit sichern?

Bleibt noch die Frage, womit die Datensicherung erfolgen soll. Grundsätzlich kann das Sichern durch einfaches Kopieren der Dateien erfolgen. Empfehlenswert ist allerdings der Einsatz sogenannter Backup-Programme, die genau für diesen Zweck entwickelt wurden.

Alle modernen Betriebssysteme enthalten ein entsprechendes Zusatzprogramm. Reicht dies für Ihre Ansprüche nicht aus, so gibt es eine Vielzahl an Produkten, die nahezu jeden möglichen Bedarf und Einsatzbereich abdecken.

Sie benötigen ein Speichermedium für die Komplettsicherung. Da in den meisten PCs CD- oder DVD/Blu-ray-Brenner eingebaut sind, eignen sich für die Speicherung der geänderten Dateien am besten Rohlinge oder wiederbeschreibbare Medien. Die heutigen Brennprogramme ermöglichen es, Daten-CDs/-DVDs oder Blu-rays zu erstellen und diese nach dem Brennen „offen“ zu lassen (Multisession). Dadurch können Sie später weitere Sicherungen auf einer solchen CD/DVD/Blu-ray speichern.

- ✓ Die Sicherung des Datenbestands beginnt mit einer Komplettsicherung. Sie erfasst alle Dateien, die Sie sichern möchten. Kennzeichnen Sie diese DVDs als Komplettsicherung.
- ✓ Haben Sie an Ihren Dateien wichtige oder umfangreiche Veränderungen vorgenommen, führen Sie die nächste Sicherung durch. Sie erfasst alle Dateien, die sich seit der letzten Komplettsicherung verändert haben. Diese Dateien speichern Sie auf der zweiten DVD, die Sie z. B. als *Sicherung-1* kennzeichnen.
- ✓ Haben Sie erneut Änderungen an Ihren Dateien vorgenommen, speichern Sie wieder alle die Dateien, die verändert wurden, auf einer dritten DVD, die Sie *Sicherung-2* nennen.
- ✓ Je nachdem, wie viele Daten Sie bei einer Sicherung speichern, verfahren Sie genauso bei den nächsten 3–5 Sicherungen.
- ✓ Nach Ablauf der von Ihnen festgelegten Zeit erstellen Sie auf einer neuen DVD eine zweite Komplettsicherung. Dadurch werden die als inkrementelle Sicherung gespeicherten Daten auf den vorherigen DVDs nutzlos. Haben Sie diese DVDs offen gelassen oder wieder beschreibbare Medien benutzt, können Sie die nächste inkrementelle Sicherung wieder auf der DVD *Sicherung-1* beginnend speichern.

Sicherungsarten

Um Benutzern eine möglichst einfache Abwicklung von Backupaufgaben zu ermöglichen, sollten Sie über die verschiedenen Sicherungsarten informiert sein, die in der IT allgemein bekannt sind:

Normale Sicherung	Jede Datei wird gesichert und durch Klicken auf <i>Vorgängerversion wiederherstellen</i> im Kontextmenü als gesichert markiert.
Kopiesicherung	Jede Datei wird gesichert, aber nicht als gesichert markiert.
Tägliche Sicherung	Jede Datei in einem ausgewählten Pfad, die das Datum des aktuellen Tages trägt, wird gesichert, aber nicht als gesichert markiert.
Inkrementelle Sicherung	Nur veränderte oder ungesicherte Dateien werden gesichert und als gesichert markiert. Der Zeitaufwand für die Sicherung ist niedriger, der für die Wiederherstellung höher als bei einer differenziellen Sicherung.
Differenzielle Sicherung	Nur veränderte oder ungesicherte Dateien werden gesichert, aber nicht als gesichert markiert. Der Zeitaufwand für die Sicherung ist höher, der für die Wiederherstellung niedriger als bei einer inkrementellen Sicherung.

Um eine Datei als gesichert zu markieren, verwendet Windows das sogenannte Archiv-Attribut. Dieses Datei-Attribut wird automatisch immer dann aktiviert, wenn eine neue Datei erstellt oder eine bestehende verändert wird. Wird eine Datei verschoben, hat dies keinen Einfluss auf Ihr Archiv-Attribut. Bei einer normalen (auch als Komplettsicherung bezeichnet) und bei einer inkrementellen Sicherung werden diese Archiv-Attribute wieder deaktiviert. Sie können ein Archiv-Attribut auch manuell verändern, indem Sie im Explorer den Kontextmenüpunkt *Eigenschaften* der betreffenden Datei auswählen, dort auf die Schaltfläche *Erweitert* klicken und das Kontrollfeld *Datei kann archiviert werden* aktivieren bzw. deaktivieren.

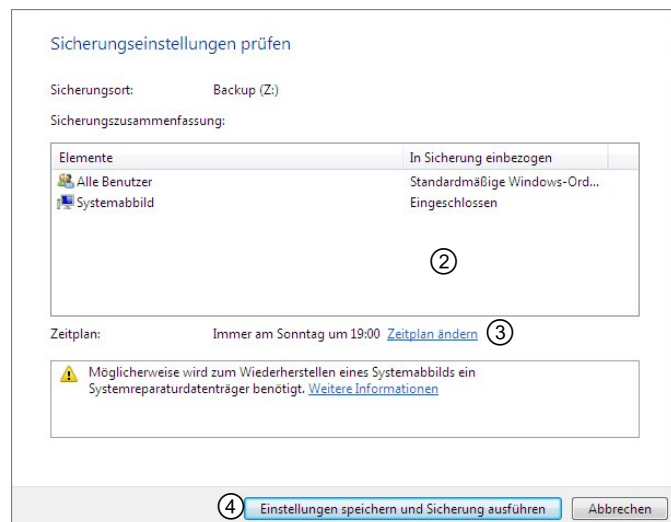
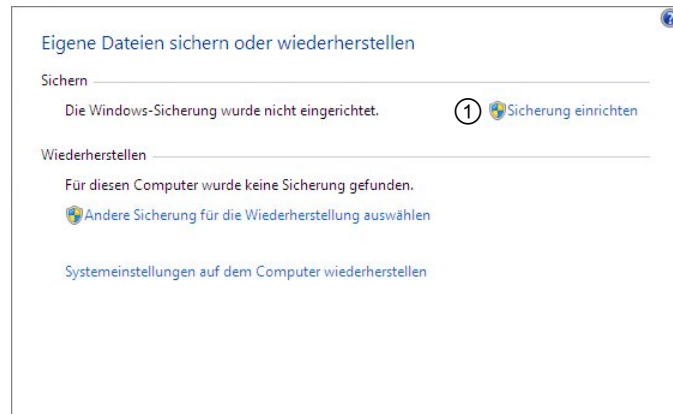
10.2 Datensicherung unter Windows 7 durchführen

Sicherung einrichten

Wenn Sie noch nie eine Sicherung durchgeführt haben, müssen Sie unter Windows 7 zunächst die Sicherungsparameter konfigurieren. Für eine effiziente Sicherungsstrategie ist es unerlässlich, in regelmäßigen Abständen die Daten zu sichern. Windows 7 unterstützt Sie bei dieser Aufgabe, indem es Ihnen die Erledigung von häufigen Aufgaben abnimmt.

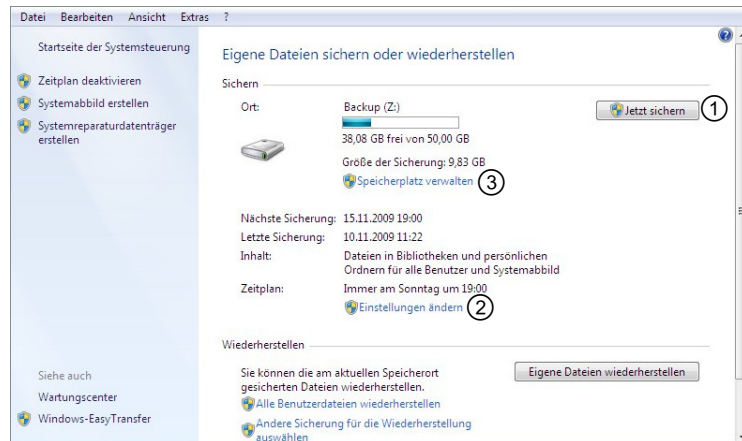
- ▶ Klicken Sie nach dem Öffnen des Startmenüs auf *Systemsteuerung* und dann auf den Link *Sicherung des Computers erstellen*.
Nun öffnet sich der Sicherungs- oder Wiederherstellungs-Assistent.
- ▶ Klicken Sie auf *Sicherung einrichten* ①.
- ▶ Wählen Sie das Sicherungsmedium, auf dem die Sicherungen gespeichert werden sollen. Je nachdem, welche Geräte an Ihrem Computer angeschlossen sind, empfiehlt sich hierfür ein DVD-Brenner, eine Sicherungsfestplatte oder die Sicherung über ein Netzlaufwerk.
- ▶ Wählen Sie als Nächstes, ob Windows entscheiden soll, welche Daten zu sichern sind, oder ob Sie selbst eine Auswahl treffen wollen. Wenn Sie eine manuelle Auswahl treffen, wählen Sie im Assistenten die zu sichernden Datenbestände aus.
- ▶ Überprüfen Sie in der Zusammenfassung, ob alle notwendigen Datenbestände in der Sicherung enthalten sind ②.
- ▶ Passen Sie den Zeitplan für eine automatische Sicherung an Ihre Bedürfnisse an ③.
- ▶ Beenden Sie den Assistenten ④.

Gleich nach dem Fertigstellen des Assistenten führt Windows 7 die erste Datensicherung durch. Dies kann je nach Datenmenge eine gewisse Zeit in Anspruch nehmen.



Manuelle Sicherung

- ▶ Klicken Sie nach dem Öffnen des Startmenüs auf *Systemsteuerung* und auf den Link *Sicherung des Computers erstellen*. Dadurch öffnet sich der Sicherungs- oder Wiederherstellungs-Assistent.
- ▶ Wenn Sie eine manuelle Sicherung durchführen wollen und die Parameter für eine Sicherung konfiguriert sind, klicken Sie auf *Jetzt sichern* ①.
- ▶ Wenn Sie Ihr Sicherungskonzept ändern möchten, klicken Sie auf *Einstellungen ändern* ②.
- ▶ Möchten Sie die Verwendung des Speicherplatzes einsehen oder die Konfiguration bezüglich der Platzverwendung ändern, klicken Sie auf *Speicherplatz verwalten* ③.



Datensicherung starten oder konfigurieren

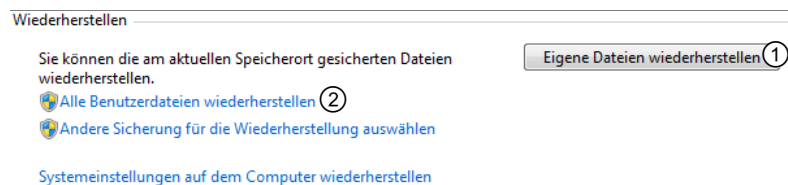
10.3 Sicherung unter Windows 7 wiederherstellen

Dateien wiederherstellen

Da Sie bei der Sicherung die Wahl haben, Ihre Daten zu sichern und zusätzlich eine Image-Sicherung (Systemabbild) der Systemlaufwerke vorzunehmen, haben Sie im Falle einer Datenpanne auch die Möglichkeit, eine Wiederherstellung anhand einer dieser beiden Methoden durchzuführen.

Sicherungsauftrag konfigurieren

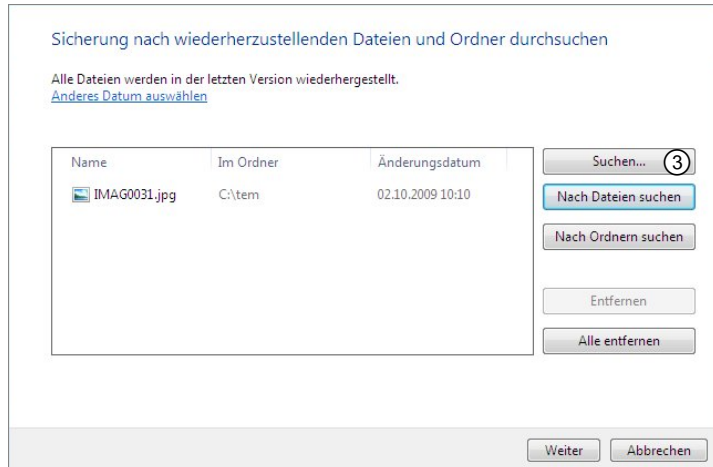
- ▶ Wenn Sie Ihre eigenen Dateien wiederherstellen wollen, klicken Sie auf die Schaltfläche ①.
- ▶ Wollen Sie als Administrator die Dateien aller Benutzer wiederherstellen, so klicken Sie auf den Link ②.



- ▶ Beantworten Sie die Fragen des Assistenten. Unter Umständen werden Sie nach dem Datum der Sicherung gefragt bzw. nach den wiederherzustellenden Dateien.
- ▶ Markieren Sie im Dateibrowser die gewünschten Dateien oder Ordner und fügen Sie diese zum Wiederherstellungsplan hinzu ③.

- ▶ Wählen Sie anschließend, ob die Dateien an ihrem ursprünglichen Ort oder einem anderen Ort wiederhergestellt werden sollen.
- ▶ Starten Sie die Wiederherstellung.

Windows Backup wird die gesicherten Dateien an den von Ihnen ausgewählten Ort kopieren und Sie nach Abschluss der Arbeiten informieren.



Dateibrowser für die Wiederherstellung

Dateien wiederherstellen in:	Beschreibung
Ursprünglicher Bereich	Dateien werden in die Laufwerke und Verzeichnisse zurückkopiert, aus denen sie entnommen wurden. Wurden die Verzeichnisse zwischenzeitlich gelöscht, werden sie wieder angelegt.
An folgendem Ort	Sie bestimmen ein Verzeichnis, in dem die Verzeichnisstruktur der gesicherten Daten wiederhergestellt werden soll.

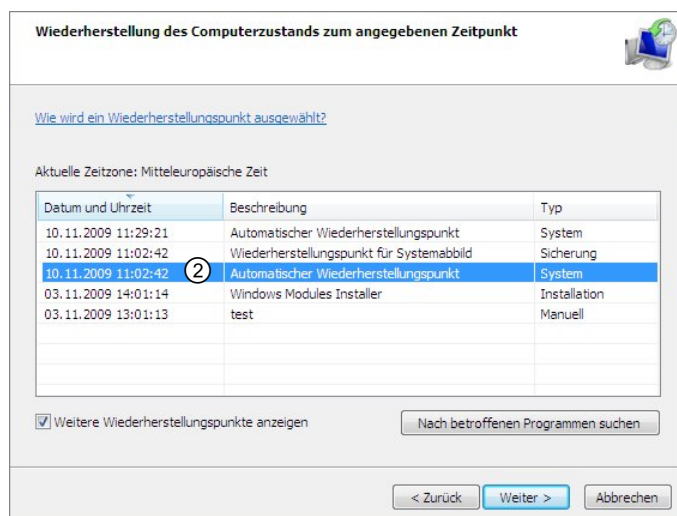
Systemwiederherstellung benutzen

Microsoft bietet im Fenster für die Wiederherstellung auch eine Systemwiederherstellung an. Falls Sie diese für einen Reparaturversuch zu Hilfe nehmen wollen, klicken Sie im Fenster *Sicherung und Wiederherstellung* auf *Systemeinstellungen auf dem Computer wiederherstellen* ①.

Im Assistenten für die Systemwiederherstellung können Sie zu einem vom Betriebssystem angelegten Systemwiederherstellungspunkt ② zurückkehren und somit eine Reparatur des Systems versuchen.



Systemwiederherstellung aktivieren



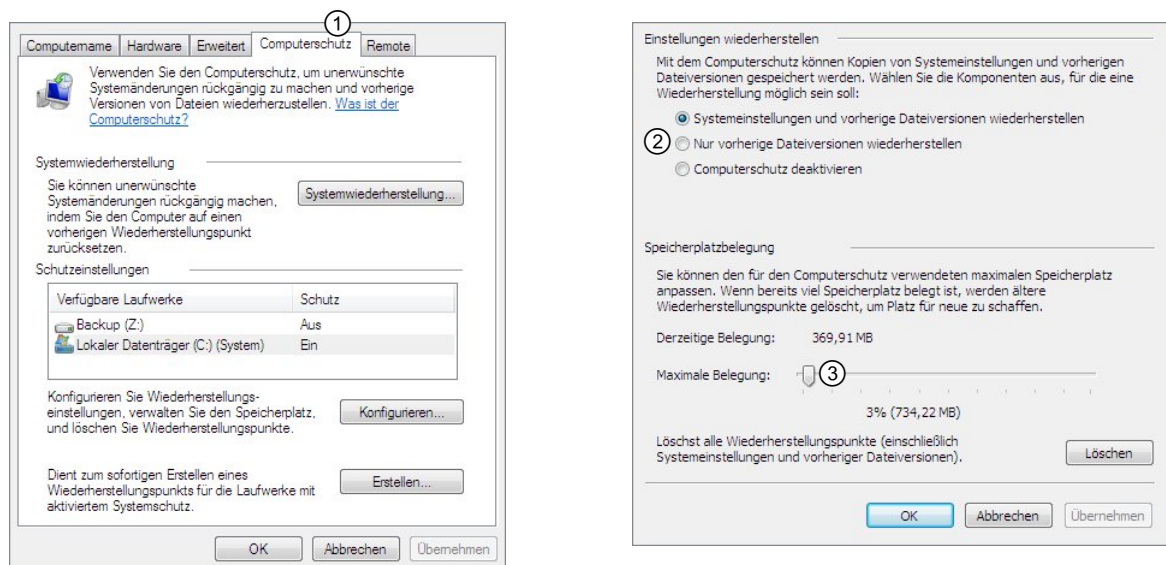
Wiederherstellungszeitpunkt auswählen

Konfigurieren der Systemwiederherstellung

Wollen Sie sich vergewissern, dass die Systemwiederherstellung gemäß Ihren Wünschen konfiguriert ist, so erreichen Sie die entsprechenden Optionen über die Eigenschaften von *COMPUTER* in der Registerkarte *Computerschutz* ①.

Sie können hier individuell pro Datenträger festlegen, ob Systemeinstellungen und Daten oder nur Daten von der Systemwiederherstellung erfasst werden, oder den Computerschutz deaktivieren ②.

Ist die Systemwiederherstellung für einen bestimmten Datenträger aktiv, können Sie auch festlegen, wie viel Speicherplatz ③ für die Sicherungsdaten verwendet werden darf.



Eigenschaften der Systemwiederherstellung konfigurieren

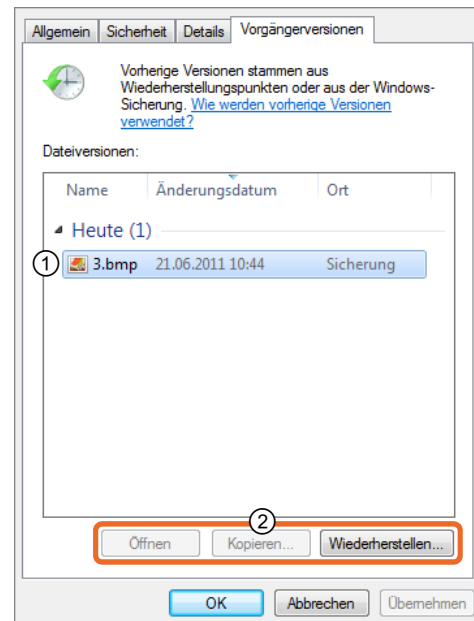
Vorgängerversion wiederherstellen

Auf die Dateisicherung, die Sie oben in der Systemwiederherstellung konfiguriert haben, können Sie mithilfe der sogenannten Vorgängerversionen wieder zugreifen.

- ▶ Wählen Sie im Kontextmenü des wiederherzustellenden Objektes den Menüpunkt *Vorgängerversionen wiederherstellen*.

Sie erhalten daraufhin ein Fenster, aus dem Sie sich die gewünschte Datei- oder Ordnerversion aussuchen ① und eine Aktion ② auswählen können.

Beachten Sie, dass Ihnen Windows 7 bei der Angabe von Vorgängerversionen sämtliche Versionen einer Datei anbietet, die entweder in der Sicherung der Systemwiederherstellung (Schattenkopien) oder in einer Windows-Sicherung enthalten sind. Sie haben somit also unabhängig von der Sicherungsart eine einheitliche Benutzeroberfläche für den Fall, dass Sie einzelne Dateien wiederherstellen möchten.



Vorgängerversionen

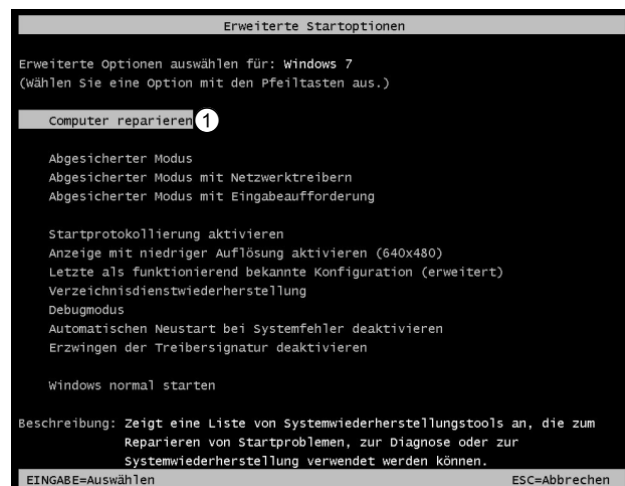
Den Computer aus einem Image wiederherstellen

Es kann vorkommen, dass die Festplatte mit der Systempartition defekt ist und Sie möglichst schnell das System mit den als Backup gesicherten Daten wieder in einen funktionsfähigen Zustand bringen müssen. In diesem Fall können Sie den Computer mithilfe des Systemabbilds schnell wiederherstellen.

- ▶ Booten Sie auf dem wiederherzustellenden Rechner von der Windows-7-Installations-CD.

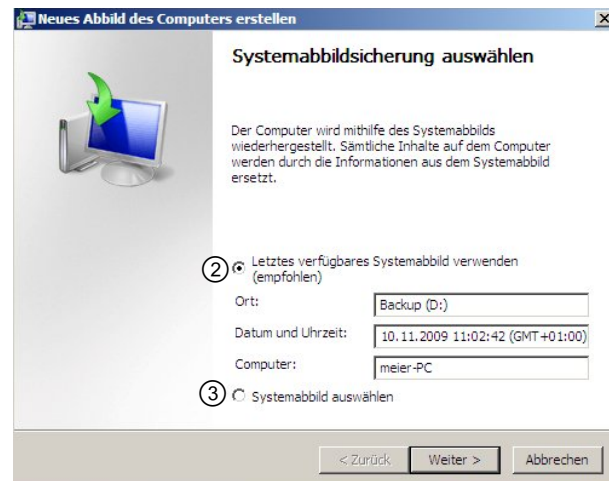
oder

- ▶ Betätigen Sie, während auf dem Bildschirm die entsprechende Meldung gezeigt wird, die Taste **F8**, um zu den Bootoptionen zu gelangen.
- ▶ Wählen Sie die Option *Computer reparieren* ①.
- ▶ Melden Sie sich als lokaler Benutzer an, um die Zugriffsrechte für eine Wiederherstellung zu erhalten.
- ▶ Wählen Sie den Link *Systemabbild-Wiederherstellung*.



Computerreparatur in den Startoptionen

- ▶ Bestätigen Sie im Assistenten anschließend die Wiederherstellung des neuesten existierenden Systemabbildes ② oder wählen Sie selbst eines der zur Verfügung stehenden aus ③.



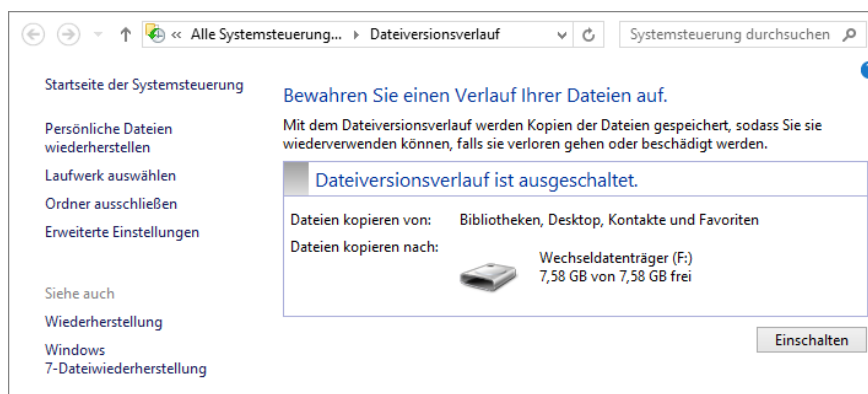
Abbild auswählen

10.4 Elemente unter Windows 8.1 und Windows 10 sichern und wiederherstellen

Sicherung von Elementen einrichten

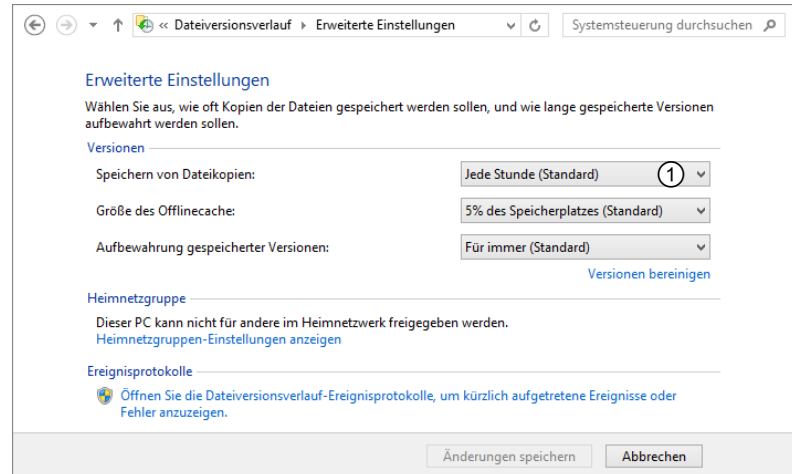
Schützen Sie Ihre Daten, indem Sie in regelmäßigen Abständen eine Sicherungskopie auf externen Speichermedien, z. B. einem USB-Stick oder einer externen Festplatte, erstellen. Standardmäßig erstellt die Desktop-App **Dateiversionsverlauf** eine Kopie aller Elemente der Bibliotheken, des Desktops, der Kontakte und Favoriten.

- ▶ Schließen Sie den USB-Stick oder eine USB-Festplatte an Ihren Computer an.
- ▶ Tragen Sie auf dem Startbildschirm die Anfangsbuchstaben *Dateiv* ein und klicken Sie auf *Dateiversionsverlauf*.
oder Geben Sie nach einem Klick auf die Startschaltfläche von Windows 10 im Suchfeld die Anfangsbuchstaben des Programmnamens (*dateiv*) ein und klicken Sie auf *Dateiversionsverlauf*
- ▶ Klicken Sie im Fenster *Dateiversionsverlauf* auf *Einschalten*, um den USB-Stick bzw. die USB-Festplatte zukünftig zur Speicherung Ihrer Elemente zu nutzen.



- ▶ Klicken Sie auf *Erweiterte Einstellungen*, um festzulegen, in welchem Zeitabstand die Elemente gesichert werden sollen.


- ▶ Wählen Sie im Fenster *Erweiterte Einstellungen* im Feld ① aus, in welchem Zeitintervall gesichert werden soll.
- ▶ Klicken Sie auf *Änderungen speichern*.
- ▶ Klicken Sie im Fenster *Dateiversionsverlauf* auf *Jetzt ausführen*, um eine Sicherung der Elemente vorzunehmen.

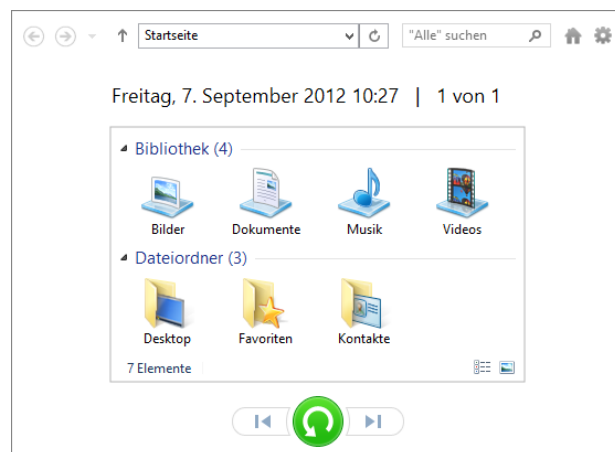


Ordner von der Sicherung ausschließen

- ▶ Klicken Sie im Fenster *Dateiversionsverlauf* auf *Ordner ausschließen*.
- ▶ Klicken Sie auf *Hinzufügen*, um einen Ordner auszuwählen.
- ▶ Wählen Sie im geöffneten Fenster *Ordner auswählen* im Inhaltsbereich den gewünschten Ordner aus.
- ▶ Bestätigen Sie mit einem Klick auf *Ordner auswählen*.
- ▶ Klicken Sie abschließend im Fenster *Ordner ausschließen* auf *Änderungen speichern*.

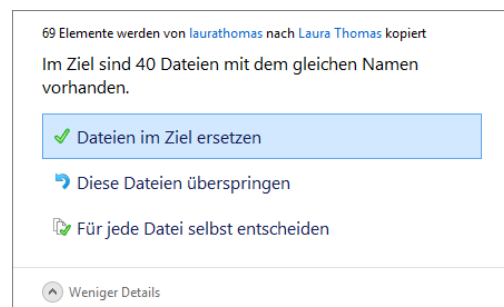
Elemente wiederherstellen

- ▶ Klicken Sie im Fenster *Dateiversionsverlauf* auf *Persönliche Dateien wiederherstellen*, um gesicherte Elemente wiederherzustellen.
- ▶ Markieren Sie durch Drücken von **[Strg]** und Anklicken die Ordner, die wiederhergestellt werden sollen.
- ▶ Klicken Sie auf , um die Wiederherstellung zu starten.
- ▶ Klicken Sie im Fenster *Dateien ersetzen oder überspringen* auf *Dateien im Ziel ersetzen*, um die vorhandenen Dateien zu überschreiben.



oder Klicken Sie auf *Diese Dateien überspringen*, um die vorhandenen Dateien beizubehalten.

oder Klicken Sie auf *Für jede Datei selbst entscheiden*, um durch Markieren und abschließendes Klicken auf *Weiter* selbst zu entscheiden, welche Datei überschrieben bzw. beibehalten wird.



10.5 Den Computer unter Windows 8.1 und Windows 10 zurücksetzen

Computer bereinigen und auf Standardwerte zurücksetzen

Falls Ihr Computer nicht mehr mit der gewohnten Geschwindigkeit arbeitet, kann dies an vorgenommenen Einstellungen, Apps und diversen Fehlern liegen. Beim Zurücksetzen des Computers werden alle vorgenommenen PC-Einstellungen sowie alle von CD/DVD und Webseiten installierten Apps entfernt. Hingegen bleiben alle Daten beispielsweise in den Bibliotheken sowie alle aus dem Store heruntergeladenen Apps erhalten.

- ▶ Legen Sie die Windows-8.1-DVD in das DVD-Laufwerk und klicken Sie in der eingeblendeten Charmleiste auf *Einstellungen*.
- ▶ Betätigen Sie in der eingeblendeten Charmleiste im unteren Bereich *PC-Einstellungen ändern*.
- ▶ Klicken Sie im Navigationsbereich *PC-Einstellungen* auf *Update/Wiederherstellung*.
- ▶ Klicken Sie im Bereich *PC ohne Auswirkungen auf die Dateien auffrischen* auf *Los geht's*.
- ▶ Betätigen Sie *Weiter* und klicken Sie auf *Aktualisieren*.

Nachfolgend wird der Computer automatisch neu gestartet und zurückgesetzt.

Um unter Windows 10 den Computer zu bereinigen oder auf Standardwerte zurückzusetzen klicken Sie im geöffneten Startmenü auf *Einstellungen* und auf *Update und Wiederherstellen* sowie danach auf *Wiederherstellen*.

Computer auf Werkseinstellung zurücksetzen

Möchten Sie den Computer neu aufsetzen, können Sie ohne großen Aufwand den Computer in den Werkszustand versetzen. Hierbei werden alle Einstellungen, Apps und Dateien gelöscht.

- ▶ Legen Sie die Windows-8.1-DVD in das DVD-Laufwerk und klicken Sie in der eingeblendeten Charmleiste auf *Einstellungen*.
- ▶ Betätigen Sie in der eingeblendeten Charmleiste im unteren Bereich *PC-Einstellungen ändern*.
- ▶ Klicken Sie im Navigationsbereich *PC-Einstellungen* auf *Update/Wiederherstellung*.
- ▶ Klicken Sie im Bereich *Alles entfernen und Windows neu installieren* auf *Los geht's*.
- ▶ Betätigen Sie *Weiter*.
- ▶ Klicken Sie auf *Nur Dateien entfernen*, um nur auf den Computer kopierte und installierte Dateien zu entfernen.
oder Klicken Sie auf *Laufwerk vollständig bereinigen*, um den Computer vollständig auf die Werkseinstellungen zurückzusetzen.
- ▶ Klicken Sie auf *Zurücksetzen*, um den Computer zurückzusetzen und neu zu starten.

Um unter Windows 10 den Computer zu bereinigen oder auf Standardwerte zurückzusetzen klicken Sie im geöffneten Startmenü auf *Einstellungen* und auf *Update und Wiederherstellen* sowie danach auf *Wiederherstellen*.

10.6 Sensible Daten endgültig löschen

Sicherheitsrisiken durch nicht vollständig gelöschte Daten

Viele Anwender wissen nicht, dass es mit entsprechenden Tools möglich ist, gelöschte Daten wiederherzustellen. Selbst Daten auf Festplatten, die neu formatiert wurden, lassen sich oftmals noch rekonstruieren.

Dies liegt daran, dass unter Windows durch das Löschen von Dateien bzw. durch das Formatieren einer Festplatte lediglich der Verweis auf die entsprechenden Dateien entfernt wird, die Daten aber nicht physikalisch vom Speichermedium entfernt werden.

Programme, die es ermöglichen, gelöschte Dateien wiederherzustellen, finden Sie beispielsweise unter folgenden Internetadressen:

- ✓ www.piriform.com/recuva
- ✓ www.pcinspector.de

Wenn Computer oder Festplatten verkauft werden oder beispielsweise durch Diebstahl in unbefugte Hände geraten, kann dies gegebenenfalls ein Sicherheitsrisiko darstellen.

Neben der Möglichkeit, Datenträger zu *shreddern* (Zerkleinerung) oder zu entmagnetisieren (*Degaussing*), existieren jedoch auch spezielle Programme, die Daten restlos beseitigen, sodass diese nicht wiederhergestellt werden können. Diese Programme löschen Daten, indem sie die entsprechenden Bereiche auf der Festplatte (mehrfach) überschreiben.

Sie finden Programme zur restlosen Beseitigung von Daten beispielsweise unter folgenden Internetadressen:

- ✓ www.gaijin.at/dlwipefile.php
- ✓ www.heidi.ie/eraser/
- ✓ www.secure-eraser.de

Anders als auf lokalen Datenträgern verhält es sich mit dem Löschen von Daten und Inhalten in sozialen Netzwerken, Blogs, Internetforen und Cloud-Services. Bei diesen Diensten bedeutet Löschen nicht automatisch, dass Daten und Inhalte endgültig vernichtet werden. Teils halten die Diensteanbieter die Daten und Inhalte dauerhaft oder für eine bestimmte Zeit vor bzw. Suchmaschinen können bereits gelöschte Daten und Inhalte immer noch abrufbar machen, da diese im sogenannten Cache der Suchmaschine gespeichert sind.

A

So finden Sie die Inhalte zu den Lernzielen

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
1	Grundbegriffe zu Sicherheit	
1.1	Datenbedrohung	
1.1.1	Zwischen Daten und Informationen unterscheiden können.	7
1.1.2	Die Begriffe Cybercrime und Hacken verstehen.	12–13
1.1.3	Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen.	8–10
1.1.4	Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben.	8–10
1.1.5	Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen, wie: Datenkontrolle, möglicher Verlust der Privatsphäre.	8–10
1.2	Wert von Informationen	
1.2.1	Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit.	8–10
1.2.2	Verstehen, weshalb personenbezogene Daten zu schützen sind, z. B. um Identitätsdiebstahl und Betrug zu verhindern, zum Schutz der Privatsphäre.	12–13 14–16
1.2.3	Verstehen, weshalb Firmendaten auf Computern und mobilen Geräten zu schützen sind, z. B. um Diebstahl, betrügerische Verwendung, unabsichtlichen Datenverlust und Sabotage zu verhindern.	12–13 14–16
1.2.4	Allgemeine Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle kennen, wie: Transparenz, Notwendigkeit, Verhältnismäßigkeit.	11
1.2.5	Die Begriffe Betroffene und Auftraggeber verstehen. Verstehen, wie die Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle für Betroffene und Auftraggeber angewendet werden.	11

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
1.2.6	Verstehen, dass bei der Nutzung von IKT die Einhaltung von Grundsätzen und Richtlinien wichtig ist; wissen, wie die Richtlinien üblicherweise bekanntgemacht werden bzw. zugänglich sind.	8–10
1.3	Persönliche Sicherheit	
1.3.1	Den Begriff Social Engineering verstehen und die Ziele kennen, wie: unberechtigter Zugriff auf Computer und mobile Geräte, unerlaubtes Sammeln von Informationen, Betrug.	14–16
1.3.2	Methoden des Social Engineering kennen, wie: Telefonanrufe, Phishing, Shoulder Surfing.	14–16
1.3.3	Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen.	14–16
1.3.4	Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming, Pretexting.	14–16
1.4	Sicherheit für Dateien	
1.4.1	Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen.	46
1.4.2	Die Vorteile und die Grenzen von Verschlüsselung verstehen. Wissen, wie wichtig es ist, das Passwort, den Schlüssel und das Zertifikat der Verschlüsselung nicht offenzulegen und nicht zu verlieren.	18–24
1.4.3	Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln.	22–23
1.4.4	Dateien mit einem Passwort schützen, z. B.: Dokumente, Tabellenkalkulationsdateien, komprimierte Dateien.	22–23
2	Malware	
2.1	Arten und Funktionsweisen	
2.1.1	Den Begriff Malware verstehen; verschiedene Möglichkeiten kennen, wie Malware auf Computern und anderen Geräten verborgen werden kann, wie: Trojaner, Rootkit, Backdoor.	43–44
2.1.2	Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm.	44–46
2.1.3	Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Botnet, Keylogger, Dialer.	43–46
2.2	Schutz	
2.2.1	Die Funktionsweise und die Grenzen von Antiviren-Software verstehen.	51–52
2.2.2	Verstehen, dass Antiviren-Software auf Computern und mobilen Geräten installiert sein soll.	51–52

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
2.2.3	Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen.	51
2.2.4	Laufwerke, Ordner und Dateien mit Antiviren-Software scannen; Zeitplan für Scans mit Antiviren-Software festlegen.	53–55
2.2.5	Verstehen, dass die Verwendung veralteter und nicht mehr unterstützter Software mit Risiken verbunden ist, wie: zunehmende Gefährdung durch Malware, Inkompatibilität.	51
2.3	Problemlösung und -behebung	
2.3.1	Den Begriff Quarantäne verstehen und die Auswirkung auf infizierte oder verdächtige Dateien kennen.	55–56
2.3.2	Infizierte oder verdächtige Dateien unter Quarantäne stellen oder löschen.	55–56
2.3.3	Wissen, dass ein Malware-Angriff mithilfe von Online-Ressourcen identifiziert und bekämpft werden kann, wie: Websites der Anbieter von Betriebssystemen, Antiviren-Software und Web-Browser; Websites von zuständigen Behörden/Organisationen.	51–52 57–58
3	Sicherheit im Netzwerk	
3.1	Netzwerke und Verbindungen	
3.1.1	Den Begriff Netzwerk verstehen und übliche Netzwerktypen kennen, wie: Local Area Network (LAN), Wireless Local Area Network (WLAN), Wide Area Network (WAN), Virtual Private Network (VPN).	29–30
3.1.2	Verstehen, wodurch sich eine Verbindung zu einem Netzwerk auf die Sicherheit auswirken kann, wie: Malware, unberechtigter Zugriff auf Daten, Schutz der Privatsphäre.	34–35 43–44 59–60 69–70
3.1.3	Die Aufgaben der Netzwerk-Administration verstehen, wie: Authentifizierung, Benutzerrechte verwalten, Nutzung dokumentieren, sicherheitsrelevante Patches und Updates überwachen und installieren, Netzwerkverkehr überwachen, Malware im Netzwerk bekämpfen.	32–33
3.1.4	Die Funktion und die Grenzen einer Firewall bei der privaten Computernutzung und in einer Arbeitsumgebung verstehen.	34–35
3.1.5	Personal Firewall ein- und ausschalten; den durch die Personal Firewall laufenden Datenverkehr für eine Anwendung, einen Dienst/Funktion zulassen bzw. blockieren.	36
3.2	Sicherheit im drahtlosen Netz	
3.2.1	Verschiedene Möglichkeiten zum Schutz von drahtlosen Netzwerken und deren Grenzen kennen, wie: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)/Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) Filter, Service Set Identifier (SSID) verbergen.	37–38

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
3.2.2	Sich bewusst sein, dass auf ein ungeschütztes drahtloses Netzwerk Angriffe erfolgen können, wie: unbefugter Zugriff durch Eindringlinge, Hijacking, Man-in-the-Middle-Angriff.	37–38
3.2.3	Den Begriff Persönlicher Hotspot verstehen.	39
3.2.4	Einen sicheren persönlichen Hotspot einschalten und ausschalten; Geräte sicher damit verbinden und trennen.	39–40
4	Zugangskontrolle	
4.1	Methoden	
4.1.1	Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, wie: Benutzername, Passwort, PIN, Verschlüsselung, Multi-Faktor-Authentifizierung.	14–16 24
4.1.2	Den Begriff Einmal-Passwort und die typische Verwendung verstehen.	14–16
4.1.3	Verstehen, wozu ein Netzwerk-Konto dient.	32–33
4.1.4	Verstehen, dass der Zugang zu einem Netzwerk-Konto mit Benutzername und Passwort erfolgen soll, und dass der Zugang bei Nichtgebrauch durch Sperren oder Abmelden geschlossen werden soll.	32–33
4.1.5	Biometrische Verfahren zur Zugangskontrolle kennen, wie: Fingerabdruck, Auge scannen, Gesichtserkennung, Handgeometrie.	25
4.2	Passwort-Verwaltung	
4.2.1	Richtlinien für ein gutes Passwort kennen, wie: angemessene Mindestlänge beachten, aus Buchstaben und Ziffern und Sonderzeichen zusammensetzen, geheim halten, regelmäßig ändern, unterschiedliche Passwörter für unterschiedliche Dienste.	23–24
4.2.2	Die Funktion und die Grenzen einer Passwort-Verwaltungssoftware verstehen.	23–24
5	Sichere Web-Nutzung	
5.1	Browser-Einstellungen	
5.1.1	Einstellungen zum Ausfüllen von Formularen aktivieren und deaktivieren, wie: automatische Vervollständigung, automatisches Speichern.	59–60 63–65 66–67
5.1.2	In einem Browser persönliche Daten löschen, wie: Browserverlauf, Downloadverlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten.	63–65
5.2	Sicheres Surfen	
5.2.1	Sich bewusst sein, dass bestimmte Online-Aktivitäten (Einkaufen, E-Banking) nur auf sicheren Webseiten über eine gesicherte Netzwerkverbindung erfolgen sollen.	60–61 65–66

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
5.2.2	Kriterien zur Beurteilung der Vertrauenswürdigkeit einer Website kennen, wie: inhaltliche Qualität, Aktualität, gültige URL, Information zum Inhaber der Webseite (Impressum), Kontaktdaten, Sicherheitszertifikat, Überprüfung der Domain-Inhaberschaft.	62
5.2.3	Den Begriff Pharming verstehen.	48–49
5.2.4	Den Zweck und die Funktionsweise von Software zur Inhaltskontrolle kennen, wie: Internet-Filterprogramme, Kinderschutz-Software.	68–69
6	Kommunikation	
6.1	E-Mail	
6.1.1	Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird.	76–81
6.1.2	Den Begriff Digitale Signatur verstehen.	76–77
6.1.3	Arglistige und unerwünschte E-Mails erkennen.	14–16
6.1.4	Typische Merkmale von Phishing kennen, wie: Verwendung der Namen von seriösen Unternehmen und Personen, Verwendung von Logos und Markenzeichen, Links zu gefälschten Webseiten, Aufforderung zur Bekanntgabe persönlicher Daten.	14–16
6.1.5	Wissen, dass Phishing-Attacken den betroffenen seriösen Unternehmen und zuständigen Behörden/Organisationen gemeldet werden können.	16
6.1.6	Sich der Gefahr bewusst sein, dass ein Computer oder mobiles Gerät mit Malware infiziert werden kann, wenn ein E-Mail-Attachment geöffnet wird, das ein Makro oder eine ausführbare Datei enthält.	52
6.2	Soziale Netzwerke	
6.2.1	Verstehen, dass es wichtig ist, vertrauliche oder personenbezogene Informationen nicht in sozialen Netzwerken zu veröffentlichen.	69
6.2.2	Sich der Notwendigkeit bewusst sein, in sozialen Netzwerken geeignete Konto-Einstellungen auszuwählen und regelmäßig zu überprüfen, wie: Privatsphäre, Standort.	69–75
6.2.3	Konto-Einstellungen in sozialen Netzwerken anwenden: Privatsphäre, Standort.	69–75
6.2.4	Mögliche Gefahren bei der Nutzung von sozialen Netzwerken kennen, wie: Cyber-Mobbing, Cyber-Grooming, bösartige Veröffentlichung persönlicher Inhalte, falsche Identitäten, betrügerische oder arglistige Links, Inhalte oder Nachrichten.	43–44 68–69
6.2.5	Wissen, dass missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken dem jeweiligen Service-Provider und zuständigen Behörden/Organisationen gemeldet werden kann.	16

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
6.3	VoIP und Instant Messaging	
6.3.1	Schwachstellen bei der Sicherheit von Instant Messaging (IM) und Voice over Internet Protocol (VoIP) verstehen und Gefahren kennen, wie: Malware, Backdoor-Zugang, Zugriff auf Dateien, Lauschangriff.	80
6.3.2	Methoden kennen, um beim Gebrauch von IM und VoIP Vertraulichkeit sicherzustellen, wie: Verschlüsselung, Nicht-Veröffentlichung von wichtigen Informationen, Zugriff auf Daten einschränken.	80
6.4	Mobile Geräte	
6.4.1	Verstehen, welche Folgen die Verwendung von Anwendungen aus inoffiziellen App-Stores haben kann, wie: mobile Malware, unnötiger Ressourcenverbrauch, Zugriff auf persönliche Daten, schlechte Qualität, versteckte Kosten.	81
6.4.2	Den Begriff App-Berechtigungen verstehen.	81
6.4.3	Wissen, dass mobile Anwendungen private Informationen von mobilen Geräten auslesen können, wie: Kontaktdaten, Standortverlauf, Bilder.	81
6.4.4	Für den Fall, dass ein mobiles Gerät abhandenkommt, Sofortmaßnahmen und Vorsichtsmaßnahmen kennen, wie: Fernsperrung, Fernlöschung, Geräteortung.	81
7	Sichere Dateiverwaltung	
7.1	Daten sichern und Backups erstellen	
7.1.1	Maßnahmen zur physischen Sicherung von Computern und mobilen Geräten kennen, wie: nicht unbeaufsichtigt lassen, Standort der Geräte und weitere Details aufzeichnen, Sicherungskabel verwenden, Zugangskontrolle.	7–10 22–26
7.1.2	Wissen, wie wichtig eine Sicherungskopie für den Fall des Datenverlusts auf Computern und anderen Geräten ist.	82–85
7.1.3	Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit/Häufigkeit, Zeitplan, Ablageort, Datenkompression.	82–85
7.1.4	Backup an einem Speicherort erstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.	82–87 91–92
7.1.5	Daten von einem Backup-Speicherort wiederherstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.	82–85 87–91 93

Modul IT-Security (gemäß Lernzielkatalog-Version 2.0)		Seite(n)
7.2	Daten sicher löschen und vernichten	
7.2.1	Den Unterschied zwischen der Löschung von Daten und der endgültigen Löschung/Vernichtung von Daten kennen.	94
7.2.2	Den Sinn und Zweck einer endgültigen Löschung/Vernichtung von Daten auf Laufwerken oder Geräten verstehen.	94
7.2.3	Sich bewusst sein, dass das Löschen von Inhalten bei manchen Diensten nicht endgültig ist, wie: Soziale Netzwerke, Blogs, Internetforen, Cloud-Dienste.	94
7.2.4	Methoden zur endgültigen Datenvernichtung kennen, wie: Laufwerke/Datenträger zerstören, z. B. schreddern; Entmagnetisierung; Software zur Datenvernichtung verwenden.	94

8

802.11i 38

A

Access-Point 34

Account 33

ActiveX-Steuerelemente 59, 62

Administrator 32

Adware 47

AES 38

Aktive Inhalte 59, 62

Antivirenprogramme 51

Asymmetrische Verschlüsselung 20

Authenticity 8

Authentifikation 8

Authentifizierung 21, 32, 59

AutoVervollständigung 66

Availability 9

avast! Free Antivirus installieren 52

avast! Free Antivirus, Quarantäne 55

avast! Free Antivirus, Warndialog 55

B

Backdoorprogramme 44

Backup 82

Backup einrichten 91

Backup wiederherstellen 92

Benutzerverwaltung 32

Betrug 43

Biometrie 25

Blockieren von Inhalten 65

Bootsekturviren 45

Botnetze 52, 57, 58

Browserverlauf löschen 64

C

Computer auffrischen 93

Computer in Werkzustand versetzen 93

Computer zurücksetzen 93

Computerbetrug 12

Computerkriminalität 12

Confidentiality 8

Cookies 59, 63, 64

Cyber-Bullying 43

Cybercrime 12

Cyber-Mobbing 43

D

Dateien mit Passwort schützen 25

Dateien und Ordner verschlüsseln 22

Dateiversionsverlauf 91

Dateiviren 45

Daten endgültig löschen 94

Datenmanipulation 12

Datenmitnahme 13

Datenschutz 59, 63

Datensicherung 82, 86

Datensicherung, Arten 85

Datensicherung, Dateien wiederherstellen 87

Datensicherung, manuelle 87

Datensicherung, Medien 87

Datensicherungsstrategien 84

DE-Cleaner 58

Demilitarisierte Zone 35

Dialer, illegale 44

Diebstahl von Daten 12

Digital signierte Nachrichten 77, 79

Digitale ID anfordern 77

Digitale ID versenden 76

Digitale Signatur 21

Digitale Zertifikate 59

DMZ 35

DNS-Flooding 49

DNS-Server 48

Drahtloses lokales Netzwerk 30

Dumpster Diving 15

E

Echtheit einer Webseite überprüfen 62

Eingeschränkte Sites, Sicherheitszone 62

Einmal-Kennwort 15

Elemente sichern 91

Elemente wiederherstellen 92

Erpressung 13

F

Facebook 69

Facebook Blocker 69

Facebook, ältere Beiträge 74

Facebook, Anwendungen und Inhalte einschränken 73

Facebook, individuelle Einstellungen zur Privatsphäre 70

Facebook, Markierungen 73

Facebook, Personen und Anwendungen blockieren 75

Facebook, Privatsphäre 70

Facebook, Sicherheits-einstellungen 73

Facebook, Standardeinstellungen für die Privatsphäre 72

Facebook, Werbung und Anwendungen 74

Firewalls 34

G

GAN 29

Gefahren im Internet 69

Gelöschte Dateien wiederherstellen 94

Geschützter Modus 63

H

Hashfunktion 21

Hijacking 48

Hotspot 39, 40

https 60

Hybride Viren/Würmer 46

I

IEEE 802.11i 38

Image wiederherstellen 90

Infektionsroutine 45

Information Diving 15

Inhalten blockieren 65

InPrivate-Funktion 65

Integrität 8

Integrity 8

Internet, Gefahren 69

Internet, Sicherheitszone 62

Internet-Mobbing 43

ISO-Norm 27002 10

IT-Sicherheit 10

J

Java-Script-Applets 62

Jugendgefährdende Inhalte 43

Jugendschutz 68

K

Kensington-Schloss 7

Keylogger 44

Keystroke Logging 44

Kinderschutz 68

Komplettsicherung 85

Komprimierte Dateien mit Passwort schützen 26

Kontakte mit Zertifikat 80

Kontenvergabe 32

Kryptoanalyse 18

Kryptografie 18

Kryptologie 18

L

LAN 29

Linkviren 45

Lokales Intranet, Sicherheitszone 62

Löschen, endgültiges 94

M		S		Vertraulichkeit	8
MAC-Filterung	37	Scareware	44	Viren, Bauplan	45
Makroviren	46	Schlüsselmanagement	19	Virens Scanner installieren	52
Malware	43	Schlüsseltausch	19	Virensuche, Einstellungen festlegen	53
MAN	29	Secure Socket Layer	60	Virensuche, Laufwerke festlegen	54
Manipulation	13	Service Set Identifier	37	Virtual Private Network	30
Mobbing	43	Shoulder Surfing	16	VLAN	30
Mobile TAN	15	Sichere Passwörter	24	VPN	30
N		Sichere Verbindungen	60	W	
		Sicherheit	7	WAN	29
Nachrichten digital signieren	77, 79	Sicherheitsprobleme	10, 13	Wardriving	37
Nachrichten verschlüsseln	77, 79	Sicherheitsprotokolle	59, 60	WaveLAN	30
Netzwerk	29	Sicherheitszertifikate	59, 60	Webseite, Zertifikat	60
Non-Repudiation	9	Sicherheitszertifikate einsetzen	76	WEP	38
Notfallspeichermedium	51	Sicherheitszonen	59, 62	Werkzustand	93
Nutzlast	45	Sicherung von Elementen	91	Wiederherstellen, gelöschte Dateien	94
O		Sicherung wiederherstellen	92	Wi-Fi	30
		Signatur, digitale	21	Windows Defender	57
Öffentlicher Schlüssel	76	Skimming	16	Windows-Firewall Apps zulassen bzw. blockieren	36
Online Social Engineering	14	Skriptviren	46	Windows-Firewall ein- bzw. ausschalten	36
Ordner von Sicherung ausschließen	92	Social Engineering	14, 46	Wired Equivalent Privacy	38
Overwrite-Infektion	45	Speicherresidente Viren	45	WLAN	30
P		Spionage	12, 13	WLAN-Verbindung	39
		Spionage-Software	43	WLAN-Verbindung trennen	40
Passwort	33	Sponsoring	47	WPA (Wi-Fi Protected Access)	38
Passwörter verwenden	23	Spyware	43, 47, 48, 57, 58	WPA2 (Wi-Fi Protected Access 2)	38
Passwörter, sichere	24	SSID	37	Würmer	46
Payload	45	SSID-Broadcast	37	Z	
Personalisierte Tracking-Schutz-Liste	65	SSL	21, 60	Zertifikat auswählen	78
Persönlicher Hotspot	39, 40	T		Zertifikat einem Kontakt hinzufügen	80
Pharming	48	TAN	15	Zertifikat, persönliches anfordern	77
Phishing	15, 43, 49	Tarnroutine	45	Zertifikate	22
Policy	10	Temporäre Internetdateien löschen	64	Zertifikate beurteilen	61
Preshared Key	38	TKIP	38	Zertifikate erstellen	77
Pretexting	14	Tracking-Schutz aktivieren	65	Zertifikate, digitale	59
Private Key	20	Trojaner	44	Zertifikate, Webseite	60
Privater Schlüssel	76	TSR	45	Zertifikatfehlermeldung	61
Privatsphäre, individuelle Einstellungen	70	U		Zertifizierungsstellen	77
Privatsphäre, Standard-einstellungen	72	Überwachung	33	Zugangskontrolle	25
Protokoll <i>https</i>	60	Umgang mit Passwörtern	23	Zugriffsrechte	33
PSK	38	Urheberrecht	11	Zugriffsschutz	32
Public Key	20, 21	V		Zuwachssicherung	85
Public Key Infrastructure	21	Verbindlichkeit	9		
Public-Key-Algorithmus	76	Verfügbarkeit	9		
R		Verschlüsseln von Nachrichten	77, 79		
Rettungs-CD	51	Verschlüsselung	18, 20		
Richtlinien zur Datenaufbewahrung	10	Verschlüsselung, asymmetrische	20		
Rootkit	44	Vertrauenswürdige Sites, Sicherheitszone	62		