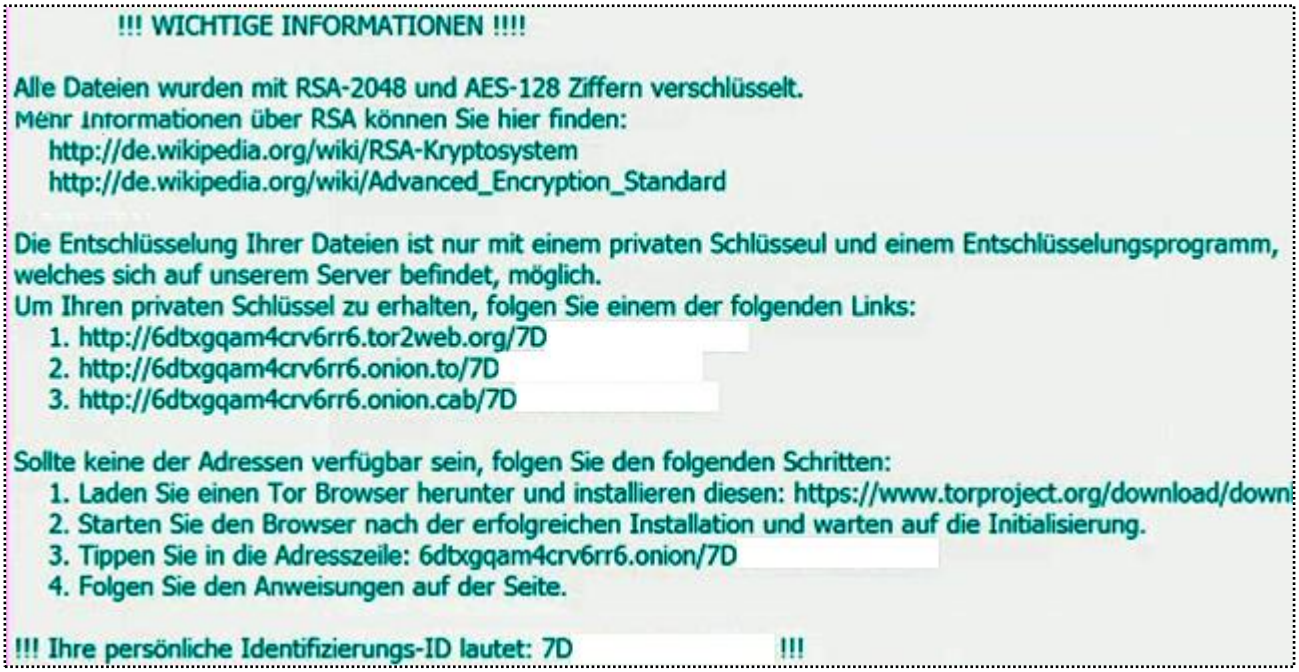
Datensicherheit

Risiken im Umgang mit Daten

- Bearbeite das Arbeitsblatt 12, S. 1: Risiken im Umgang mit Daten (Wiederholung)

Datenverlust
Wenn dein PC nach dem Start nicht mehr den gewohnten Desktop anzeigt, sondern nur noch diese oder ähnliche Informationen preisgibt, ist es passsiert:



Die Dateien auf dem Datenträger des PC wurden durch den Verschlüsselungstrojaner *Locky verschlüsselt*. Der Trojaner zeigt Details zu dem Verschlüsselungsverfahren an und verweist auf Internetadressen, unter denen beschrieben wird, wie das Lösegeld zu bezahlen ist, um den Schlüssel zu erhalten.
Auch Fachleuten wird eine Entschlüsselung nicht gelingen. Die einzige Möglichkeit, **eventuell** wieder an seine Daten zu gelangen, besteht darin, das Lösegeld zu zahlen. Davon rät das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) allerdings ab (Stand: Dezember 2016), denn:

- Es ist nicht sichergestellt, dass die Entschlüsselung auch gelingt.
- Wenn Erpresser Erfolg haben, werden sie und Nachahmer ermutigt, die Straftat zu wiederholen.

Das BSI rät weiterhin, die Erpressungsnachricht zu fotografieren und Anzeige zu erstatten. Man kann die Daten auch aufbewahren und hoffen, dass die Verschlüsselung irgendwann geknackt wird.

- Die sinnvollste Maßnahme gegen jede Art von Datenverlust ist **Prävention**: Anfertigen eines *Backups* (einer Sicherungskopie) der Daten.

Was bedeutet aber *Verschlüsselung von Informationen*?

- Bearbeite das Arbeitsblatt 12, S. 2: Verschlüsselung von Informationen

- **Kryptographie** ist die Wissenschaft, die sich mit Informationssicherheit befasst, also u. a. mit der *Verschlüsselung* von Informationen. Das *Entschlüsseln* von Informationen bezeichnet man als **knacken**.
- Die Verschlüsselung ist **nicht** grundsätzlich etwas Schlechtes – **im Gegenteil**: Ursprünglich wurde sie entwickelt, um **Daten vor unbefugtem Zugriff zu schützen**. Du wirst später noch erfahren, dass auch deine Daten durch Verschlüsselung geschützt werden. Hier wird lediglich ein sinnvolles Verfahren von Kriminellen umgekehrt und als Mittel zum Begehen von Straftaten eingesetzt.

Die Gefahr, dass Daten verloren gehen, ist aber nicht nur durch Verschlüsselungstrojaner gegeben. Viel häufiger sind technische Defekte oder Benutzerfehler Ursachen für Datenverluste.

A Bearbeite das Arbeitsblatt 12, S. 4: Datenverlust

Datenträger
Die Lebensdauer digitaler Datenträger ist begrenzt.

- Bei Festplatten und SSDs kann jederzeit ein **technischer Defekt** auftreten.
- Datenträger können auch durch eine größere Katastrophe wie z. B. einen **Brand** zerstört werden.
- Daten können auch durch **natürliche Alterung** und weitere Faktoren verloren gehen. Oft kann man nur vermuten, wie lange Datenträger lesbar bleiben. Natürlich gibt es auch große Schwankungen.

  Die Angaben in der Tabelle unten sind nur grobe Richtwerte. In Klammern sind Faktoren angegeben, die die Lebensdauer verringern. Wenn Daten wirklich wichtig sind, sollte man nicht annähernd so lange warten wie unten angegeben ist, sondern viel früher neue Kopien der Daten anfertigen.

Festplatten (Stöße, Magnetismus)	○ im laufenden Betrieb ca. 2 bis 10 Jahre (Wärmeschwankungen) ○ als Archivmedium: mindestens 10 Jahre
Optische Speichermedien (Wärme, Licht, Feuchtigkeit und Kratzer)	○ gebrannte **CD-R** bzw. **DVD**: im laufenden Betrieb 5–10 Jahre, als Archivmedium vermutlich mindestens 30 Jahre ○ gepresste **CD**: vermutlich etwa 50-80 Jahre ○ gepresste **DVD**: vermutlich mindestens 100 Jahre
Flash-Speicher (Anzahl der Schreibzyklen in TBW (Terabyte Written))	○ **SSD** oder **USB-Speicherstick**: im laufenden Betrieb in Abhängigkeit der TBW einige Jahre ○ als Archivmedium: unbekannt; sehr lange
Cloud-Speicher (Angriffe von außen, der Anbieter stellt den Dienst ein)	○ theoretisch unbegrenzt

- Archivierte Daten müssen in regelmäßigen Abständen neu kopiert werden!
- Bei SSDs sollte die Anzahl der TBW regelmäßig kontrolliert werden. Die Hersteller bieten dafür Tools an, wie beispielsweise Samsung Magician:

  Die Hersteller garantieren derzeit zwischen 60 und 150 TBW (Stand: Dezember 2016).
  Allerdings vertragen die SSDs tatsächlich normalerweise viel mehr Schreibzyklen. Nach einem Test (vgl. c't 2017, Heft 1, S. 100-103) zwischen knapp 200 und über 4000 TBW.
- Insbesondere billige USB-Speichersticks sind für das Archivieren von Daten **nicht** empfehlenswert, weil hier oft minderwertiger Flash-Speicher verwendet wird.

Spionage
Daten gelangen auf vielfältigen Wegen in die Hände von Dritten, die diese Daten missbrauchen können. Ein möglicher Weg ist Schadsoftware auf Geräten des Benutzers (vgl. Arbeitsblatt 1.8-12, S. 5, *Einfallstore*).

- Typische Programme zur Spionage sind:
  - **Spyware** sendet Daten eines Benutzers ohne dessen Wissen an einen Empfänger.
  - **Sniffer** zeichnen den Datenverkehr eines Netzwerks auf, um gesendete Daten wie beispielsweise Passwörter auszuspionieren.
  - Besonders gefährlich sind **Keylogger**, die Tastatureingaben kontrollieren und damit Passwörter mitlesen, bevor sie verschlüsselt werden können.
- Ein möglicher Weg ist z. B. auch **Dumpster Diving**: Hier wird Abfall nach vertraulichen Informationen durchsucht, um das Vertrauen des Opfers gewinnen und ihn betrügen zu können. Oft werden aber auch direkt vertrauliche Daten wie z. B. Kontodaten oder Passwörter durch achtlos weggeworfene Zettel gefunden (z. B. Banküberweisungsbelege).
- Vertrauliche Benutzerdaten gelangen aber auch regelmäßig durch **Hacking** bei Internetanbietern in die Hände Unbefugter. Durch solche **Datenlecks** wurden in den vergangenen Jahren Milliarden von Zugangsdaten erbeutet. Sie werden von Kriminellen „genutzt", bevor sie dann im Darknet verkauft und später auch veröffentlicht werden. Bis die Nutzer dann erfahren, dass ihre Daten missbraucht werden konnten, dauert es aber oft mehrere Jahre.

A Bearbeite das Arbeitsblatt 12, S. 5: Spionage und Angriffsziele

Angriffsziele
Lange Zeit hielt sich hartnäckig das Gerücht, das wären alles nur Probleme für Windows-PCs. Tatsächlich sind logischerweise besonders weit verbreitete Systeme für Kriminelle am lohnendsten, weil sie hier mit demselben Aufwand mehr Angriffsziele haben als bei irgendwelchen Nischenprodukten.

- Alle hier genannten Merkmale gelten aber nicht nur für Computer, sondern für **alle Geräte, die mit dem Internet verbunden sind!**

Missbrauch von Daten
Warum ist es so wichtig, sensible Daten möglichst vor dem Zugriff durch Dritte zu schützen?
Nicht umsonst wurden im Jahr 2016 beispielsweise gestohlene Zugangsdaten zu einem einzigen Konto für das Sony Playstation Network im Darknet für über 10 Euro verkauft (vgl. c't 2016, Heft 23, S. 79).

- **Identitätsdiebstahl** ist die missbräuchliche Nutzung personenbezogener Daten einer Person, z. B.:
  - Direkter Betrug mit Kreditkarten oder Bankkonten wie Bezahlungen oder Überweisungen.
  - Tätigen von Geschäften unter Verwendung der fremden Identität, z. B. Einkäufe.
  - Ermitteln weiterer personenbezogener Daten im Namen des Opfers (z. B. Konto-, Krankheits- oder Versicherungsdaten), um mit vervollständigten Datensätzen dunkle Geschäfte machen zu können.
  - Veröffentlichungen (z. B. in sozialen Netzwerken oder Blogs), um eine Person in Misskredit zu bringen. Hier sind auch Folgetaten wie Erpressung möglich.
- **Personenprofile, Scoring und Rasterung**: Durch die Nutzung des Internets fallen immer *mehr* sowie immer *vielfältigere* Daten immer *schneller* an. Dabei entstehenden relativ zufällige „Datenschnipsel" (z. B. Verbindungsdaten oder Ortsdaten), die zu Datensätzen zusammengestellt und ausgewertet werden. Das wird als *Big Data* bezeichnet. Die Ergebnisse dienen Organisationen und Unternehmen zum Erstellen von Prognosen z. B. zur Steuerung von Forschung, Entwicklung und Werbung.
  - Ein wichtiger Beitrag daraus zur Verbesserung der Lebensverhältnisse wäre z. B. das frühzeitige Erkennen von Epidemien, also ansteckenden Massenerkrankungen.
  - Die Datensätze sind aber auch personalisierbar, lassen sich also einem Internetnutzer zuordnen. Dadurch entstehen Personenprofile, die verblüffend genau sind. Dennoch sind auch viele Fehler enthalten. Schon alleine der Handel mit personenbezogenen Daten ist bedenklich. Gefährlich wird es, wenn sich fehlerhafte Datensätze aus automatisierten Datenverarbeitungsvorgängen negativ auf einzelne Personen auswirken, z. B. bei der Bewerbung um einen Arbeitsplatz, bei der Auswahl einer Krankenversicherung oder bei der Kreditvergabe durch Banken.

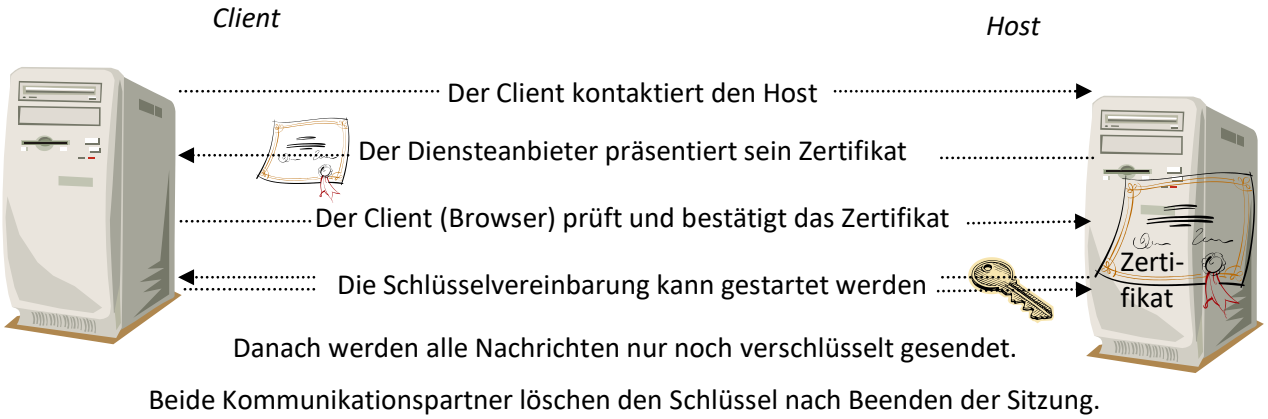
A Bearbeite das Arbeitsblatt 12, S. 6: Missbrauch von Daten

Maßnahmen zur Datensicherheit

A Bearbeite das Arbeitsblatt 13, S. 1: Wiederholung von Grundlagen der Kommunikation im Internet

Verschlüsselung der Kommunikation im Internet

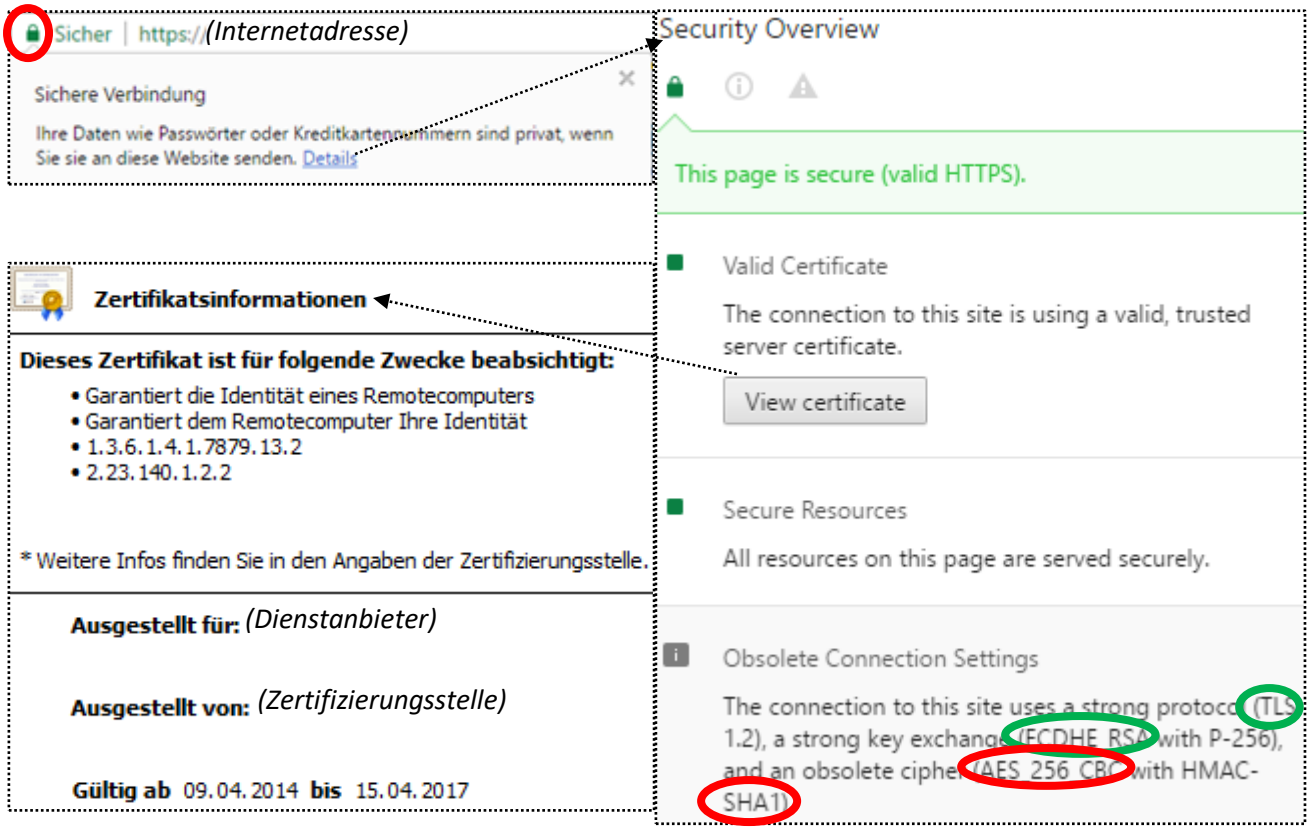
Um sicherzustellen, dass der Partner auch derjenige ist, für den er sich ausgibt, verfügt der Host über ein **Zertifikat** (*Authentifizierung*). Zertifikate werden von unabhängigen Zertifizierungsstellen ausgestellt. Das Zertifikat enthält auch Informationen zum Verschlüsselungsverfahren. Das läuft dann so ab:



Danach werden alle Nachrichten nur noch verschlüsselt gesendet.

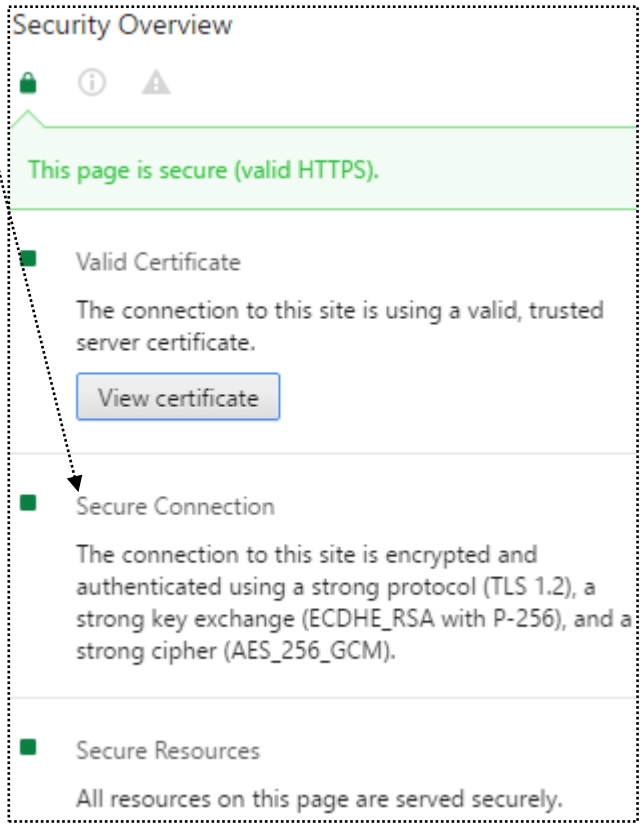
Beide Kommunikationspartner löschen den Schlüssel nach Beenden der Sitzung.

Wenn man im Browser das Schlosssymbol einer https-Verbindung anklickt, wird je nach Browser eventuell nur eine banale Information wie „Ihre Verbindung mit dem Server ist verschlüsselt“ eingeblendet. *Opera* und *Mozilla Firefox* geben etwas mehr Informationen zu dem verwendeten Verschlüsselungsverfahren preis. Derzeit erhält man in *Google Chrome* die detailliertesten Informationen (Stand: 03.01.2017):



Wenn man sich aber nicht auf die Einschätzung von Google verlassen, sondern sich eine eigene Meinung bilden will, kann man auch die verwendeten Verfahren in unabhängigen Quellen recherchieren.

Am 08.01.2017, also fünf Tage später, wurden die Verschlüsselungsverfahren der Website im Beispiel vorne gut bewertet (siehe Abbildung rechts), was den schnellen technischen Wandel aufzeigt.



Es gibt es unterschiedliche Protokolle und Verfahren für die verschlüsselte Kommunikation.
Das Prinzip ändert sich zwar kaum, aber technische Details relativ schnell, weil die Einschätzung der Sicherheit mit der Geschwindigkeit von Computern, mit denen die Verschlüsselung geknackt werden kann, Schritt halten muss.
Das gilt nicht nur für die Internetanbieter, sondern auch für die Browserversion, die du verwendest.

- Mit einem veralteten Browser kann kein aktueller Sicherheitsstandard gewährleistet werden.

Was bedeuten aber die Angaben unter „Connection“?

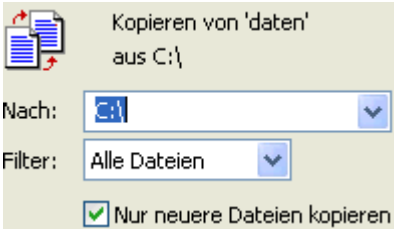
- **TLS** (**T**ransport **L**ayer **S**ecurity) ist ein Protokoll zur verschlüsselten Datenübertragung im Internet. Dabei handelt es sich um eine Weiterentwicklung des **S**ecure **S**ockets **L**ayer (**SSL**).
  Die Bezeichnung SSL wird noch häufig synonym zu TLS verwendet.
  Wenn dieses Protokoll verwendet wird, besteht eine verschlüsselte Verbindung.
  Ob die Verbindung aber wirklich sicher ist, hängt von der Chiffriermethode (Cipher-Suite) ab.
  Diese beinhaltet:
  - Das Verfahren zum **Schlüsselaustausch** („key exchange“):
    - Bei der **asymmetrischen Verschlüsselung** im Beispiel (**ECDHE**_RSA) erzeugen beide Partner ein eigenes Schlüsselpaarauf Basis elliptischer Kurven nach Diffie-Hellman. Dieses Verfahren ist stark, weil kein gemeinsamer Schlüssel existiert, der berechnet oder übermittelt wird.
      Es ist nur schwer und auch im Nachhinein nicht mehr zu knacken – wenn die Schlüssel wie vorgesehen nach Beendigung der Sitzung sofort gelöscht werden.
    - Um sicherzustellen, dass der Kommunikationspartner auch derjenige ist, der er vorgibt zu sein (Authentifikation), wird RSA verwendet (ECDHE_**RSA**).
    - Da die asymmetrische Verschlüsselung nicht sehr schnell ist, wird sie nur dafür verwendet, eine **symmetrische Verschlüsselung** auszuhandeln, die dann für die weitere Kommunikation verwendet wird, den *Sitzungsschlüssel* (hier: **AES_256_GCM**). Dann verwenden beide Partner denselben Schlüssel, der aber vorher über einen sicheren Kanal ausgetauscht werden muss.
      Der „Cäsar-Code“ vorne war ein ganz einfaches Beispiel für ein symmetrisches Verfahren.
- **SHA** (**S**ecure **H**ash **A**lgorithm) wird bei SSL standardmäßig eingesetzt, um die Vollständigkeit und Echtheit einer Nachricht (Integrität) zu überprüfen.
  SHA1 wird nicht mehr empfohlen (vgl. vorige Seite).
  Hier sollte derzeit zumindest **SHA2** zum Einsatz kommen (Stand: Januar 2017).

A Bearbeite das Arbeitsblatt 13, S. 2: Verschlüsselung der Kommunikation im Internet

Dateiarchivierung (Backup)

Zur Archivierung kann man Dateien entweder einfach auf andere Datenträger kopieren oder mit Hilfe von Archivierungssystemen zwischen unterschiedlichen Datenträgern abgleichen.

Die Bordmittel der aktuellen Betriebssysteme (z. B. Explorer) sind dafür nur bedingt geeignet.



Z. B das Programm Speed Commander enthält die Option „nur neuere Dateien kopieren“.

- Ein ganz einfaches Mittel, aktualisierte Dateien zu kopieren, bieten z. B. **Dateiverwaltungswerkzeuge**. Hier genügt schon der unscheinbare Schalter „nur neuere Dateien kopieren“, um ganze Verzeichnisbäume komfortabel abgleichen zu können. Wenn auf einen USB-Datenträger archiviert wird, stehen so mit geringer Handarbeit jederzeit und überall die aktuellen Versionen der Dateien zur Verfügung. Außerdem hat man die volle Kontrolle über den Kopiervorgang.
- Eine andere Möglichkeit ist der Abgleich mit Hilfe von **Synchronisationsprogrammen**. Dabei werden zuvor festgelegte Aktionen automatisch ausgeführt. Das ist bequemer als das Kopieren von Hand, dafür müssen die Backupoptionen zuvor festgelegt werden. Außerdem ist die Gefahr von Benutzerfehlern größer: Das versehentliche Löschen von Dateien wird genauso synchronisiert wie das Erstellen einer neuen Datei – die Datei wird also auch in der Sicherungskopie gelöscht.
  Gute Clients zur Dateisynchronisation bieten deshalb auch eine Versionsverwaltung an, die einen Schutz vor Benutzerfehlern bietet. Hier werden ältere Versionen der Dokumente aufbewahrt.
  Bei Onlineangeboten muss man sich Gedanken zum Datenschutz machen: Die Dateien werden auf Servern gespeichert, die nie hundertprozentig gegen Angriffe geschützt sind!

Für die Archivierung von Dateien gibt es grundsätzlich zwei Möglichkeiten mit unterschiedlichen Techniken:

- **Lokale Sicherung** auf externen Datenträgern:
  - Mit einer externen USB-Festplatte am PC.
  - Langsamer, aber nach der Einrichtung etwas komfortabler in der Handhabung ist es, eine externe Festpatte mit dem Router zu verbinden. Die Anmeldedaten für die Freigabe sollten aber am PC nicht gespeichert werden, weil sonst auch Schadprogramme Zugang zu dem Datenträger haben.
  - Mit einem NAS (Network Attached Storage) für die Speicherung von Dateien im Lokalen Netz.
- **Webbasierte Sicherung**, für die verschiedene Anbieter Webspace anbieten, der oft bis zu einem bestimmten Volumen auch kostenlos vergeben wird.
  - Cloud-Speicher bieten ebenfalls oft eine Versionsverwaltung an, so dass man auf ältere Versionen der Dateien Zugriff hat. Das hilft gegen durch Verschlüsselungstrojaner unlesbar gemachte Dateien, weshalb man darauf bei der Auswahl eines Cloud-Speichers achten sollte.
  - Hier ist auch Schutz vor Katastrophen wie einem Wohnungsbrand gegeben.
  - Bei Bedenken zu dem Schutz der Daten vor Zugriffen durch Dritte können die Dateien auch zuerst lokal verschlüsselt werden.

Beide Möglichkeiten lassen sich natürlich kombinieren. Man sollte sich auf webbasierte Synchronisation alleine ohnehin nicht verlassen: Onlineanbieter behalten sich gerne in ihren AGBs vor, Benutzerkonten aus diversen Gründen einfach zu löschen.

- Eine dritte Möglichkeit ist die Kopie kompletter Datenträger entweder als Kopie oder als Abbild (Image) auf einem anderen Datenträger. Dieses Verfahren wird z. B. zur Sicherung und Verteilung von Betriebssysteminstallationen verwendet und eignet sich nicht so sehr für die Dateiarchivierung.

Zusammenfassend bieten sich für die Datensicherung die folgenden Möglichkeiten.

- Dateien lokal oder webbasiert kopieren
- Dateien lokal oder webbasiert synchronisieren
- Images von Datenträgern erstellen

➔ Am sinnvollsten ist es, mehrere Backup-Verfahren zu kombinieren.

A Bearbeite das Arbeitsblatt 13, S. 3: Dateiarchivierung

Virenschutz

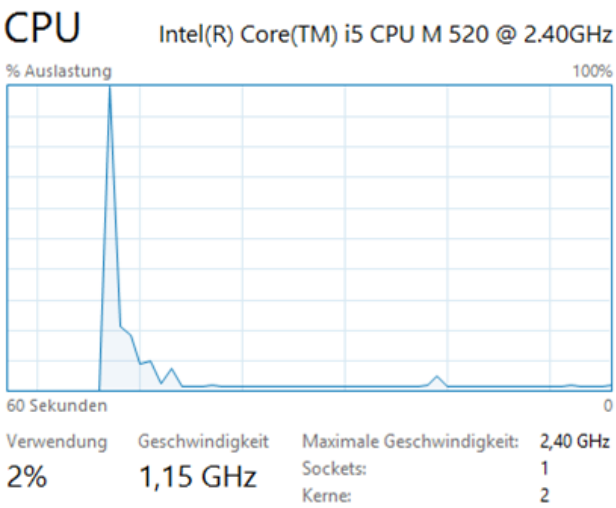
A Bearbeite das Arbeitsblatt 13, S. 4-5: Schadprogramme

Virenschutzprogramme versuchen, Computerviren, Computerwürmer und Trojaner aufzuspüren und zu beseitigen. Zuverlässig erkannt werden aber nur bekannte Schadprogramme.

- Deshalb ist es besonders wichtig, das Virenschutzprogramm stets aktuell zu halten.
  Es bietet sich an, **Produktupdates automatisch** herunterzuladen und zu installieren.
  (*siehe Konfiguration des Virenscanners*)
- Die Programme bieten auch einen Echtzeitschutz an. Hier versuchen sie, Schadprogramme bereits während des Kommunikationsvorgangs zu erkennen und zu beseitigen. Da dies aber nicht immer gelingt, sollte regelmäßig eine Systemprüfung durchgeführt werden. Dabei wird der Arbeitsspeicher und die Festplatte nach Schadprogrammen durchsucht.

Ein **Virenbefall** kann sich unterschiedlich äußern, z. B.:

- Der Virenscanner meldet einen Fund.
  Ein Fund bedeutet nicht automatisch, dass sich ein Schadprogramm eingenistet hat.
  Es gibt auch Fehlalarme.
- Das Virus macht sich bemerkbar.
  (z. B. durch Anzeigen einer Meldung)
- Dateien mit doppelter Dateiendung.
- Veränderte Dateigrößen.
- Der Virenscanner ist nicht mehr aktiv.
- Ein unbekanntes Programm bringt Meldungen und fordert dich auf, einen Button anzuklicken.
- Nicht sehr aufschlussreich ist es, wenn das Betriebssystem seltsame Meldungen bringt oder häufig abstürzt. Ein Blick in den Task-Manager (vgl. Arbeitsblatt 1.8-09, S. 3) hilft etwas weiter.
  Wenn die CPU-Auslastung ständig über 10 Prozent pendelt, obwohl du gerade keine anderen Anwendungen ausführst, stimmt vermutlich etwas nicht (siehe Abb. unten).

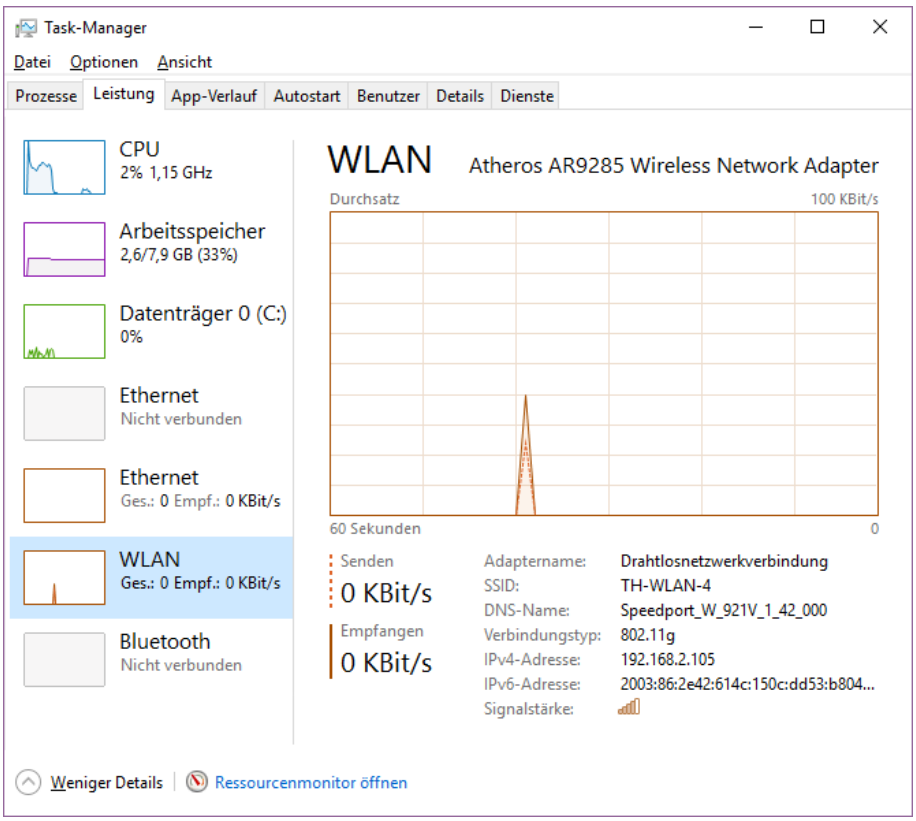


Bei dem konkreten Verdacht, dass ein Schadprogramm aktiv ist, z. B. wenn eine entsprechende Meldung erscheint:

➢ Den Computer nicht herunterfahren, sondern sofort ausschalten (durch langes Drücken der Einschalttaste) und nicht wieder einschalten, sondern sachkundigen Rat einholen.

Ein Computer sollte im Normalfall nicht hart ausgeschaltet werden, weil das zu Datenverlusten führen kann.
Das ist nur für den Notfall zu empfehlen!

Noch etwas weniger eindeutig ist das Beobachten der Auslastung des WLANs und der Festplattenaktivität: Wenn hier ständige Zugriffe erfolgen, kann das auch auf ein Programm hindeuten, das im Hintergrund arbeitet. Es könnte z. B. gerade ein Windows-Update heruntergeladen bzw. installiert werden.



Unter Android ist das nicht so komfortabel. Es gibt zwar in den Entwickleroptionen eine Einstellung, die CPU-Auslastung anzuzeigen, das ist aber recht umständlich. Es gibt auch Apps wie z. B. *System Monitor*, die einfacher handzuhaben sind und mehr Informationen bieten.

Bei einem Virenbefall sollte man auf keinen Fall in Panik ausbrechen. Beachte die folgenden Hinweise:

- Das Antivirenprogramm frägt nach, wie mit dem Virus verfahren werden soll.
- Wenn das Schadprogramm entfernt werden konnte, muss unbedingt nach einerm Neustart des Systems ein erneuter Virenscan durchgeführt werden – viele Schädlinge wehren sich gegen das Entfernen, indem sie ein Backup des Programmcodes erneut installieren.
- Wenn das Programm das Virus nicht entfernen kann, bieten die Hersteller oft auch eine Option wie *Offline prüfen* an. Dabei wird Windows im abgesicherten Modus neu gestartet und überprüft. Das kann zum Erfolg führen, weil in diesem Modus viele Schadprogramme nicht aktiv sind.
- Wenn auch das nichts hilft, sollte man den Computer mit einem sauberen Betriebssystem von einem externen Datenträger booten. Bei einigen Virenschutzprogrammen wird eine bootfähige Notfall-CD mitgeliefert, ausgerüstet mit einem Linux-Live-System und dem Virenscanner. Computerzeitschriften enthalten auch dann und wann Werkzeuge, um ein solches Live-System mit freien Virenscannern zu erstellen. Man kann von dort aus die Festplatte untersuchen und weitere Maßnahmen einleiten:
  - Mit etwas Glück gelingt es dem Virenscanner, das Schadprogramm jetzt zu entfernen.
  - Wenn man über ein aktuelles *Backup* der Systempartition verfügt, kann man dieses zurückspielen.
  - Windows legt unregelmäßig Kopien von Systemdateien an, so genannte *Schattenkopien*. Mit Hilfe eines geeigneten Tools kann man Windows auf einen Zeitpunkt vor der Infektion zurücksetzen. Das funktioniert aber nur, wenn man den Rechner schnell genug ausgeschaltet hat, bevor das Schadprogramm die Schattenkopien gelöscht hat.
  - Beim Löschen einer Datei werden nicht die Daten gelöscht, sondern nur die Einträge in der FAT. Mit Hilfe eines *Datenrettungsprogramms* kann die Festplatte nach Dateien durchsucht werden, um diese wiederherzustellen, wenn sie noch nicht überschrieben wurden. Das kann also auch nur dann funktionieren, wenn man den Rechner schnell genug ausgeschaltet hat.

A Bearbeite das Arbeitsblatt 13, S. 6: Virenschutz

Benutzerkennungen und Passwörter
Die Kombination aus Benutzername und Kennwort ist für die Anmeldung an elektronischen Geräten üblich.

- Für die Nutzung des eigenen Computers sollte eine Benutzerkennung mit eingeschränkten Rechten angelegt werden. Sofern der Administratorzugriff mit einem sicheren Passwort geschützt ist, sind somit auch die Möglichkeiten von Schädlingen eingeschränkt.
  Administratorrechte sind nur für manche Installationaufgaben erforderlich.

Zur Anmeldung bei Internetdiensten ist die Kombination aus E-Mail Adresse und Passwort weit verbreitet. Durch deren Nutzung werden unweigerlich Daten des Anwenders gespeichert. Damit wird die Wahrscheinlichkeit erhöht, dass persönliche Daten in fremde Hände gelangen, denn laufend werden Anbieter gehackt und Benutzerdaten gestohlen.
Kennwörter werden heutzutage zwar *gehasht*, sind also nicht im Klartext lesbar:

- Ein **Hash-Wert** ist das Ergebnis einer mathematischen Berechnung auf der Basis einer Zeichenkette. Dadurch werden Kennwörter unlesbar gemacht und die Korrektheit von Nachrichten überprüft.
  Das Prinzip ist ganz ähnlich wie bei der Verschlüsselung, allerdings mit zwei großen Unterschieden:
  - Der Hash-Wert hat immer dieselbe Länge, unabhängig davon, aus wie vielen Zeichen ein Passwort ursprünglich bestand.
  - Im Gegensatz zur Verschlüsselung soll der Hash-Vorgang nicht wieder rückgängig gemacht werden können. Er muss aber wiederholbar sein, denn bei der Anmeldung gibt der Nutzer sein Kennwort im Klartext ein. Dieses Kennwort muss mit dem gespeicherten Hash-Wert verglichen werden. Wer im Besitz des Berechnungsverfahrens ist, kann so ein Passwort indirekt herausfinden, denn wenn der gespeicherte Hash-Wert berechnet wird, wurde das richtige Passwort eingegeben.

  Information darüber, wie Kennwörter gehasht werden, erhält man nicht. Was den Hash-Algorithmus für Kennwörter angeht, muss man dem Anbieter vertrauen. Wenn dieser besonders sorgfältig mit den Benutzerdaten umgeht, verschlüsselt er die Kennwörter nach dem Hashen noch zusätzlich.

Viele Nutzer verwenden aber dasselbe Kennwort bei vielen Diensten. Mit Hilfe gestohlener Zugangsdaten können Kriminelle so das Kennwort herausfinden und Angriffe auf die Daten bei anderen Diensten starten. Man kann sich auch nicht darauf hinausreden, dass man ja ohnehin keine wichtigen Daten gespeichert hat: Durch unzureichend gesicherte E-Mail-Accounts und PCs wird Kriminellen, die mit Hilfe fremder Identitäten Spams verteilen oder Botnetze aufbauen wollen, das Handwerk einfach gemacht.
Passwörter müssen einerseits sicher sein, andererseits muss man sich auch eine ganze Reihe verschiedener Passwörter merken können.
Nicht sicher sind Passwörter, die sich aus einem Wort mit vorangestellten oder angehängten Ziffern oder Sonderzeichen zusammensetzen wie z. B. *Superpasswort92* oder *@Bello05*.

- Man sollte nicht für alle Zwecke dasselbe Passwort verwenden.
- Benutzerkennungen und Passwörter sollten nie unverschlüsselt gesendet werden.
- Es gibt **Passwortmanager**, die Passwörter erstellen und in Datenbanken verwalten.
- Ein Kennwort sollte möglichst lang sein und sollte Zahlen, Satz- und Sonderzeichen beinhalten. Groß- und Kleinbuchstaben sollte gemischt werden.

Abgesicherte Login-Verfahren
Achte darauf, ob Anbieter besser abgesicherte Login-Verfahren anbieten als nur die Kombination aus E-Mail Adresse und Kennwort, z. B.:

- PIN über Tastatur, zusätzliche PIN mit Maus schützt gegen Keylogger.
- Benutzerkennung (nicht E-Mail Adresse) mit PIN; zusätzlich eTAN für Transaktionen.
- Zwei-Faktor-Authentifizierung durch SMS-Code auf das Handy oder ein mit einer App generiertes Einmal-Passwort (z. B. bei Facebook, Google, Microsoft, PayPal).
- Multifaktor-Authentifizierung mit biometrischen Daten, z. B. Fingerabdruck, Iris-Scan, Stimmprobe.
- Zertifikat für den Benutzer, das in einer Datei oder in einer App auf dem Smartphone gespeichert wird, oder noch besser auf einem speziell dafür eingerichteten einem USB-Speicherstick.

A Bearbeite das Arbeitsblatt 14, S. 1: Vergabe sicherer Passwörter

Sicherheitsregeln im Umgang mit Daten

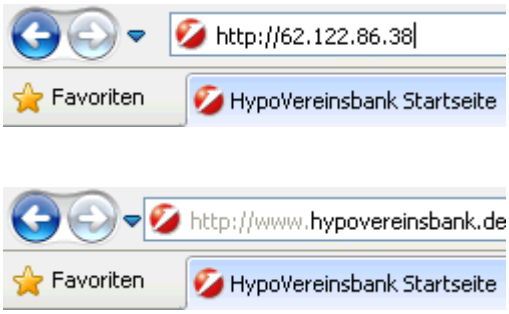
Verschlüsselung

Einzelne Dateien (vgl. Arbeitsblatt 1.8-14, S. 1) und auch ganze Datenträger wie z. B. ein USB-Speicherstick oder eine SSD können verschlüsselt werden.

- Im Internet sollten Daten nur verschlüsselt übertragen werden.
  Das erhöht die Sicherheit enorm. (*siehe Seite 4-5*)
  Der Link, der angezeigt wird, wenn du die Maus auf den *Anmelden*-Button bewegst, sollte mit einem **https://** beginnen.
  Nach erfolgtem (oder gescheitertem) Login muss dann die Internetadresse ebenfalls mit einem **https://** beginnen.

- Übermittle keine persönlichen Daten zu Internetseiten, bei denen entweder
  - keine verschlüsselte Übertragung stattfindet oder
  - als Internetadresse nur die IP-Adresse (Internet Protokoll – Adresse) eingetragen ist:

  Jeder Rechner im Internet ist unter einer Adresse bekannt, die mit einer Telefonnummer vergleichbar ist. Nach Eingabe einer Internetadresse wie z. B. www.hypovereinsbank.de wird in Wirklichkeit eine Verbindung zu dem Rechner mit der IP-Adresse http://62.122.86.38 hergestellt.
  Wenn die Internetadresse des Zielrechners nicht ersichtlich ist, kann das auf einen Täuschungsversuch hindeuten, weil die IP-Adressen schlecht zu merken sind. Im Beispiel rechts ist allerdings eine korrekte IP-Adresse angegeben.



- Dabei ist auch auf Adress-Namensverfälschungen zu achten! Durch Austausch eines Zeichens können gefälschte von echten Adressen kaum unterschieden werden (z B. www.*hypoverelnsbank.de*).
- Achte auch bei E-Mails auf sichere Verschlüsselungsverfahren!
  - Einige deutsche E-Mail-Provider (z. B. T-Online, GMX und Web.de) senden E-Mails untereinander verschlüsselt. Die Verbindung vom Client zum Server ist ohnehin per HTTPS verschlüsselt.
  - Außerdem bieten die E-Mail-Provider eine Option an, mit der E-Mails direkt auf den Geräten der Benutzer ver- und entschlüsselt werden.
    Damit ist der Inhalt der E-Mail unterwegs zu keiner Zeit im Klartext lesbar. Dafür wird die Browser-Erweiterung *Mailvelope* auf dem Gerät installiert. Dann müssen sich die beiden Partner einmalig authentifizieren, indem sie sich gegenseitig zu der verschlüsselten Kommunikation einladen. Sie erhalten einen Wiederherstellungscode, mit dem sie die Verschlüsselung aktivieren können.

- In unverschlüsselten oder unsicher verschlüsselten **WLAN**s keine vertraulichen Daten wie Passwörter senden! Der Schlüsselaustausch mit ECDHE kann zwar im Nachhinein nicht mehr geknackt werden. Ein Krimineller kann sich aber in die Kommunikation einklinken, sich gegenüber dem Client und dem Host jeweils als deren Kommunikationspartner ausgeben und ein weiteres Schlüsselpaar erzeugen. Ein solcher **man-in-the-middle-Angriff** erfordert deutlich mehr Know How als das Phishing, für das man sich lediglich im Darknet einen Trojaner und E-Mail Adressen besorgen muss, um dann ein paar E-Mails zu schreiben und darauf zu warten, dass jemand den Dateianhang mit dem Trojaner öffnet. Man-in-the-middle-Angriffe werden aber praktiziert und damit ist auch diese Verschlüsselung nicht vollkommen sicher – wenn sich der Kriminelle in eine unverschlüsselte Kommunikation wie z. B. in einem WLAN einklinken kann.

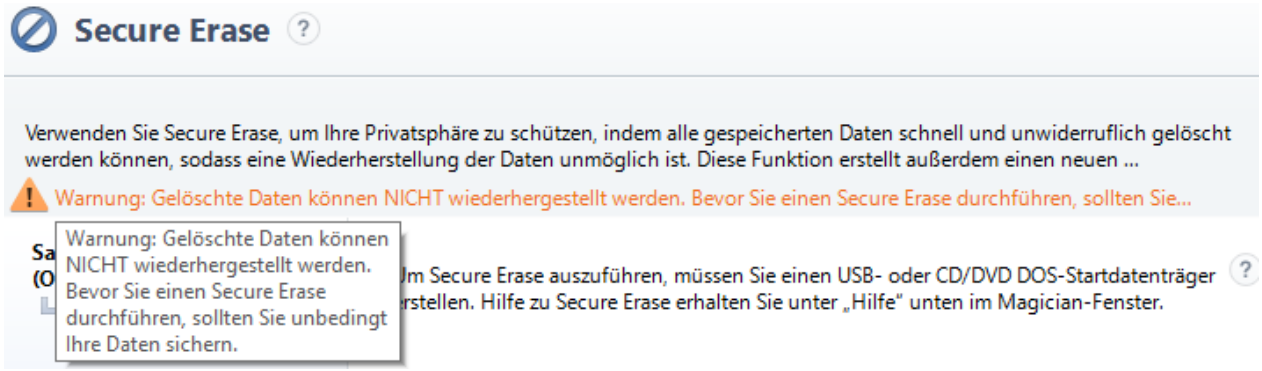
Software

- **Virenschutzprogramme**: Angeboten werden kostenpflichtige und (für private Nutzung) kostenlose Virenscanner, die als Basisschutz besser sind als kein Virenschutzprogramm. Grundsätzlich verfügen Virenschutzprogramme über zwei Möglichkeiten, Schadprogramme zu erkennen:
  - Virenscanner erhalten Informationen zu Schädlingen über Virensignaturen. Auf dieser Basis kann man einen **Virenscan** ausführen, bei dem wahlweise nur bestimmte Verzeichnisse oder alle Datenträger auf typische Muster bekannter Schadprogramme durchsucht werden.
  - Bei dem **Echtzeitschutz** findet eine laufende Überprüfung des Arbeitsspeichers und von Dateien beim Lesen oder Schreiben statt. Bei dieser Methode ist die Erkennungsrate niedriger, weshalb trotzdem regelmäßig Virenscans durchgeführt werden sollten.

  Es kann aber Stunden oder sogar Tage dauern, bis die Virenschutzprogramme die Signatur eines neuen Schädlings erhalten. Manche Virenschutz-Programme können deshalb Schadprogramme auch an ihrem Verhalten erkennen und blockieren. Das funktioniert teilweise, aber nicht perfekt und kann natürlich auch zu Fehlalarmen führen.
- Eine **Firewall** blockiert Zugriffe auf das eigene Gerät. Dadurch wird die Sicherheit erhöht, weshalb die Firewall auf jeden Fall aktiviert sein sollte.
  Um manche Dienste nutzen zu können, muss man aber den Zugriff erlauben. Dadurch entsteht eine Lücke in der Firewall. Überlege Dir also gut, ob Du ein Onlinespiel wirklich benötigst und erlaube auf keinen Fall den Zugriff einer Tauschbörse!
  - Firewall auf dem Gerät und dem WLAN-Router aktivieren bzw. aktiviert lassen!
  - Freigaben nur wohl überlegt erteilen!
  - Freigaben sofort wieder löschen, wenn sie nicht mehr benötigt werden.
- **Updates**: Software ist grundsätzlich fehleranfällig. Dadurch entstehende Sicherheitslücken werden für Angriffe auf Computersysteme genutzt. Programme werden deshalb ständig gepflegt und können mit **Updates** aktualisiert werden, die meist über das Internet zum Download angeboten werden.
  - Viele Programme – Anwendungsprogramme und Betriebssysteme – bieten die Option, Updates automatisch zu installieren. Diese Option ist meist empfehlenswert und sollte insbesondere für das Betriebssystem, für den Browser und für den Virenscanner aktiviert werden.
  - Nicht oder nicht mehr benötigte Softwaresollte man deinstallieren. Dadurch verringert man die Angriffsfläche und den Aufwand, die Software auf dem aktuellen Stand zu halten.
- Nicht nur am PC sollten regelmäßig Updates installiert werden, die Sicherheitslücken schließen. Die **Firmware aller elektronischen Geräte** sollte auf evtl. erforderliche **Updates** hin beobachtet werden. Oft erhalten Geräte durch Firmware-Updates auch zusätzliche Funktionen.
- **Datenschutzeinstellungen**
  - Bei Einstellungen wie *Feedback* und *Diagnose* im Betriebssystem werden Daten an den Hersteller gesendet und evtl. sogar der Zugriff auf den eigenen Rechner erlaubt. Im Virenscanner kann das „Übermittlung von Beispielen“ heißen oder „Cloudbasierter Schutz“.
  - Assistenten wie Cortana, Siri, Google Now oder Alexa sind anfangs ganz spaßig. Man sollte sich aber gut überlegen, ob sie es einem Wert sind, dafür die Angriffsfläche für den Missbrauch von Daten zu erhöhen.
  - Den Zugriff auf sensible Daten wie Positionsdaten, Kontaktdaten oder Kalender nach Möglichkeit nicht erlauben, wenn dies nicht wirklich erforderlich ist.

Datenträger

- Beim Löschen von Dateien werden **nicht die Daten gelöscht**, sondern lediglich die Einträge für die Dateien in der Dateizuordnungstabelle (vgl. Lerninhalte 1.8-02, S. 9 und Arbeitsblatt 1.8-08, S. 5). Ebenso werden beim Formatieren einer Festplatte nicht die Daten gelöscht. Es wird lediglich eine neue Dateizuordnungstabelle (FAT) erstellt. Die Daten können mit einfachen Tools wiederhergestellt werden, wenn sie noch nicht überschrieben wurden.
- Werden Datenträger entsorgt oder verkauft, muss deshalb unbedingt beachtet werden:
  - Ausrangierte Datenträger mechanisch zerstören bzw. wenn möglich vorher löschen!
  - Dafür kann man ein Werkzeug wie z. B. „Secure Erase“ in Samsung Magician anwenden, das die Daten sicher löscht:



Nur wenn die Datenträger komplett verschlüsselt waren (nicht nur einzelne Dateien), ist das Löschen nicht erforderlich. Smartphones und Tablets sollten in diesem Fall auf die Werkseinstellungen zurückgesetzt werden, bevor man sie abgibt. Dadurch werden die Schlüssel überschrieben.

Identitätsdiebstahl

Erhält man eine E-Mail mit dem Hinweis, dass Unregelmäßigkeiten beim Zugriff auf das Konto festgestellt worden seien, muss das noch lange nichts heißen:

- Zuerst die Authentizität der E-Mail überprüfen. Solche E-Mails sind meistens Angriffsversuche!
- Auf keinen Fall einem Link in der E-Mail folgen.

Vielleicht sind dir auch selbst seltsame Vorgänge aufgefallen. Eventuell hast du Spam-Mails erhalten, in denen korrekte personenbezogene Daten verwendet wurden? Im schlimmsten Fall bist du tatsächlich Opfer eines Identitätsdiebstahls geworden.
Es gibt Möglichkeiten, das zu überprüfen, z. B. unter den Internetadressen

- Unter `https://www.sicherheitstest.bsi.de/` kann man seine E-Mail Adresse angeben, um festzustellen, ob bei dem *Bundesamt für Sicherheit in der Informationstechnik* Informationen zu einem möglichen Identitätsdiebstahl vorliegen.
- Datensätze von Nutzern gehackter Internetanbieter werden im Darknet verkauft. Nach einiger Zeit sind solche Datensätze meist auch öffentlich im Internet zugänglich. Wenn man den Verdacht hat, dass ein Account bei beinem Portal geleakt (von *Leak*, englisch für Leck, undichte Stelle) wurde: Auf der Webseite `haveibeenpwned.com` kann man abfragen, ob ein Account mit der eigenen E-Mail-Adresse aus einem Datenleck bereits öffentlich zugänglich ist (engl. *powned* – auf deutsch *erwischt*). Der Dienst gibt die Anzahl der Datensätze derzeit mit über zwei Milliarden an (Stand: 03.01.2017).

- Erhält man eine positive Rückmeldung: Zumindest bei allen Onlinediensten, bei denen man dasselbe Kennwort oder Passwortschema nutzt, dieses dringend ändern oder den Account löschen!
- Erhält man keine Rückmeldung, bedeutet das keineswegs Entwarnung. Man sollte weiterhin wachsam sein und eventuell trotzdem vorsorglich Zugangsdaten bei Onlinediensten ändern.

A Bearbeite das Arbeitsblatt 14, S. 2: Checkliste