



## 2.5.2 Datennetze II

### Web 2.0

1. Beschreibe die Unterschiede zwischen den beiden Versionen des Textverarbeitungsprogramms.

2.5.2-Datennetze-II

Lerninhalte-01-Milestones-der-Entwicklung-des-Internets-und-ihre-gesellschaftliche-Bedeutung

Im Verlauf des ersten Jahrzehnts des 21. Jahrhunderts fanden zwei weitere wichtige Entwicklungen statt: Es wurde zunehmend von dem Web 2.0 und dem IoT (Internet of Things, dt. Internet der Dinge) gesprochen.

A→Bearbeite das Arbeitsblatt 03, S. 1-2: Web 2.0

➤ Der Begriff „Web 2.0“ bzw. „Social Media“ wurde im Zusammenhang mit zunehmender Interaktivität des Internet (Cloud Computing) geprägt, z.B.:  
o→ **Groupware**: Dabei handelt es sich um Anwendungen, mit denen gemeinsames Arbeiten in einer Gruppe unterstützt wird. Dazu gehört z.B.:  
o→ **Teamfunktionalität** in Officeprogrammen, damit mehrere Benutzer an einem Dokument arbeiten können. Damit entfällt die bis dahin erforderliche Verwaltung verschiedener Versionen desselben Dokuments. Dokumente werden nicht lokal,

Wiktionary

Wikt[ənəri] Das freie Wörterbuch

Mit mir geht's - OneDrive

Word Online

DATEI START EINFÜGEN SEITENLAYOUT ÜBERPRÜFEN ANSICHT Was möchten Sie tun?

252-01-lerninhalte.docx

Freigaben

V.

Jeder mit dem Link kann anzeigen und bearbeiten.

Namen oder E-Mail-Adresse eingeben

Nachricht hinzufügen (optional)

Senden

- I. Die Datei wird **auf einem Server im Internet** gespeichert.
  - II. Die Datei wird **lokal** gespeichert.
  - III. Die Programoberfläche wird **in einem Browser** angezeigt, die Anwendung wird **auf einem Server** ausgeführt.
  - IV. Die Anwendung ist **auf einem PC** installiert.
  - V. Das Textdokument kann **von mehreren Benutzern** gleichzeitig bearbeitet werden.
  - VI. Das Textdokument kann **nur von einem Benutzer** bearbeitet werden.
- Früher war eine Anwendung immer auf einem lokalen Rechner installiert. Beim **Cloud Computing** wird Speicherplatz und Anwendungssoftware im Internet genutzt. Im „**Web 2.0**“ können Benutzer Daten im Internet zur Verfügung stellen, direkt zusammenarbeiten und kommunizieren.



## 2.5.2 Datennetze II

2. Beschreibe die Merkmale eines Wikis:  
(siehe Abbildung rechts)

*Lösungsvorschlag:*

*Jeder registrierte Benutzer kann Inhalte veröffentlichen und bearbeiten.  
Damit wird das Wissen vieler Nutzer zusammengefasst und vernetzt.*

The screenshot shows the homepage of Wiktionary (https://de.wiktionary.org/wiki/Wiktionary). The page title is "Wiktionary, das freie Wörterbuch". It features a sidebar with links like "Hauptseite", "Themenportale", "Zufällige Seite", "Inhaltsverzeichnis", "Mitarbeiter", "Eintrag erstellen", "Autorenportal", "Wunschliste", "Literaturliste", "Letzte Änderungen", "Hilfe", "Drucken/exportieren", "Buch erstellen", "Als PDF herunterladen", and "Druckversion". The main content area displays statistics: "658.062 deutschsprachige Einträge zu über 230 Sprachen" and a section titled "Allgemeine Hinweise" with tips for entry creation.

3. Bei einem **Blog** („Weblog“) handelt es sich um ein öffentlich einsehbares Tagebuch. Die Leser können meist Diskussionsbeiträge ergänzen, so dass im Blog auch Kommunikation möglich ist. Beispielsweise in *Twitter* können Kurznachrichten verfasst werden.
- Rufe einen Blog auf. Wähle z. B. eine prominente Person aus der Politik, aus dem Showgeschäft oder aus dem Sport. Lies und bewerte einige Beiträge.
4. Nenne Vorteile von **Instant-Messaging-Diensten** wie *Skype* oder *WhatsApp* gegenüber *SMS* oder *E-Mail*.

*Z. B.: Audio- und Videotelefonie oder Gruppenchats sind möglich.*

*Seit einigen Jahren gibt es Ende-zu-Ende-Verschlüsselung.*

5. Über **Soziale Netzwerke** wie *Facebook*, *XING* oder *LinkedIn* können sich Benutzer vernetzen. Nenne Gründe für die Nutzung der unterschiedlichen Sozialen Netzwerke.

*XING: Herstellen und vernetzen geschäftlicher bzw. beruflicher Kontakte.*

*Facebook: Private Kontakte – aber auch Organisationen, die private Nutzer ansprechen oder Empfehlungen von Nutzern (Werbung) einholen.*

The screenshot shows the homepage of XING (https://www.xing.com). It features a search bar at the top and two main sections: "Stellenmarkt" (Job Market) and "Unternehmen" (Companies). Each section has a circular icon and a brief description. Below these are two paragraphs of text.

Stellenmarkt: Finden Sie den Job, der zu Ihrem Leben passt und lassen Sie sich automatisch über neue Angebote informieren.

Unternehmen: Finden Sie die besten und beliebtesten Arbeitgeber mit Top-Bewertungen in Ihrer Stadt oder für Ihre Branche.

The screenshot shows the homepage of Facebook (https://de-de.facebook.com). It features a search bar at the top and a large blue header with the word "facebook". Below the header is a promotional text: "Auf Facebook bleibst du mit Menschen in Verbindung und teilst Fotos, Videos und vieles mehr mit ihnen."

- Der Begriff „**Social Media**“ beinhaltet, dass sich Benutzer im Internet vernetzen können.
- Das beinhaltet, Inhalte einfach veröffentlichen und gemeinsam bearbeiten können.
  - Damit kann das gemeinsame Wissen von Nutzern zusammengefasst und vernetzt werden.
  - Wissen, Meinungen und andere Informationen werden schnell verbreitet.



## 2.5.2 Datennetze II

### „Dinge“ in Netzwerken

In privaten Privathaushalt werden immer häufiger unterschiedliche Geräte mit einem WLAN vernetzt. Oft funktioniert das Lokale Netz ohne weitere Anpassungen. Fraglich ist nur, ob die Standardeinstellungen des WLAN-Routers sinnvoll sind und was zu tun ist, wenn doch nicht alles wie gewünscht funktioniert.

- Im Beispiel (vgl. Arbeitsblatt 2.5.1–07, S. 2-3) wurde ein Twisted-Pair- Kabel in das Arbeitszimmer gelegt und dort eine Ethernet-Anschlussdose installiert.

\* Erstellt mit Sweet Home 3D.

Das Programm ist veröffentlicht unter der GNU General Public License.

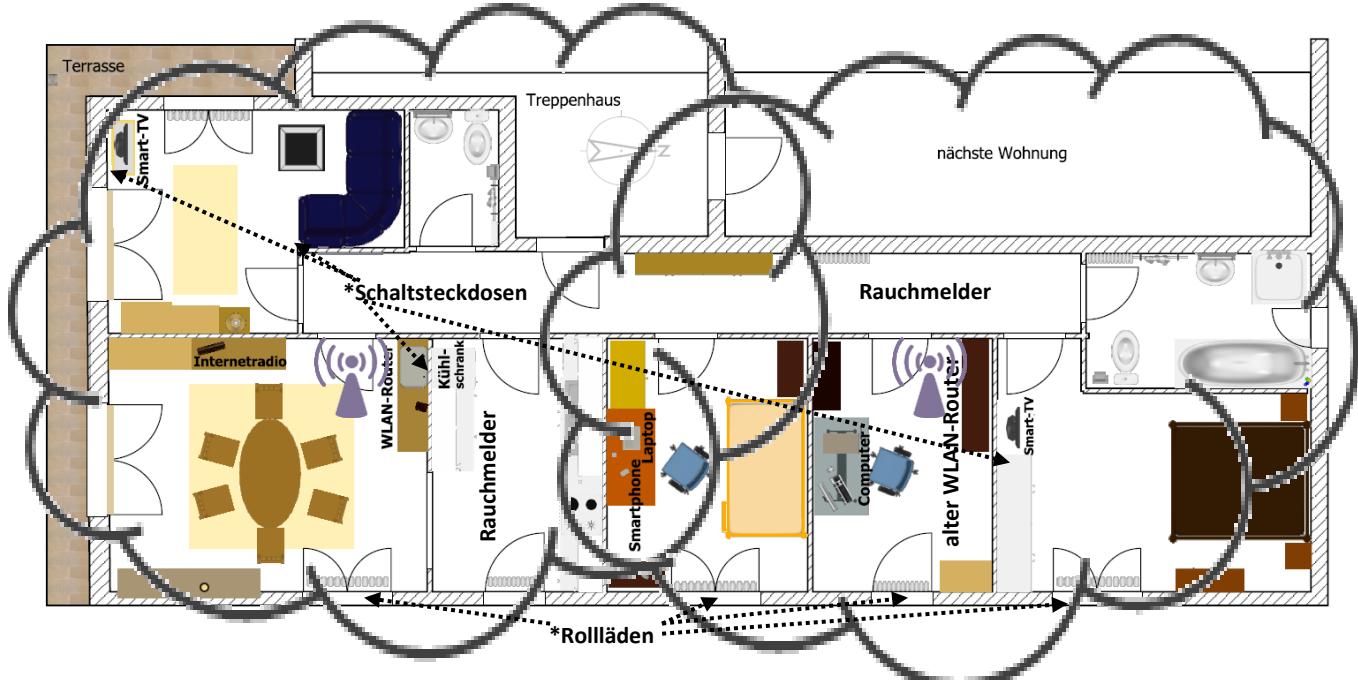
Weitere Informationen und Download: <http://www.sweethome3d.com/>

Hinweise (Wiederholung):

- Da der WLAN-Router der Ausgangspunkt möglicher Maßnahmen ist, wird dieser vergrößert dargestellt.
- Durch Hindernisse wird das Funksignal gedämpft. Eine Mauer reduziert die Signalstärke je nach Dicke der Wand etwa um ein Viertel. Feuchtigkeit und Metall dämpfen besonders stark. Das gilt z. B. für mit Metallträgern gebaute Rigipswände, Fußbodenheizungen, Waschmaschinen oder Kühlschränke.
- Die Signalstärke ist im Bereich von 2-3 Wänden normalerweise hinreichend, wobei die Datenübertragungsrate mit jeder Wand immer weiter abnimmt.
- Der WLAN-Router steht auf der anderen Seite der Wand direkt hinter dem Kühlschrank. Allgemein gilt: Je höher der Router steht, desto besser. In diesem Fall sollte er auf jeden Fall über dem Kühlschrank montiert werden, wofür man ein Wandregal anbringen könnte.
- ➔ An dem Computer im Arbeitszimmer kann man das WLAN-Signal evtl. noch empfangen, an dem Smart-TV im Schlafzimmer aber auf keinen Fall mehr.

Da ein alter WLAN-Router übrig war, musste kein WLAN Access Point gekauft werden. Die beiden WLAN-Router lassen sich einfach über die Ports ihrer Switches verbinden.

Außer den **weiteren Smarthome-Komponenten\*** ist noch ein Saugroboter vorhanden.





## 2.5.2 Datennetze II

### Sicherheitslücken

„**Massiver DDoS auf weite Teile des Internets**“ – Dienste wie Twitter, Netflix, Spotify und PayPal waren teilweise nicht erreichbar. Grund war ein Distributed-Denial-of-Service-Angriff mit Hilfe des Mirai-Botnetzes, „das zum großen Teil aus gehackten Geräten aus dem Internet der Dinge (IoT) wie Kameras und smarten Haushaltsgeräten besteht.“ (c't 2016, Heft 23, S. 39)

6. Mit Hilfe gekaperter Geräte werden **Botnetze** aufgebaut. Diese können für **DDoS-Angriffe** genutzt werden („Distributed Denial of Service“; dt. „Verbreitete Verweigerung des Dienstes“). Dabei werden Datennetze durch Überlastung lahmgelegt. Die arglosen Nutzer, deren Geräte für das Botnetz missbraucht werden, ahnen nichts davon, dass sie an einer kriminellen Aktion beteiligt sind. Auch zurückverfolgen lassen sich die Angriffe praktisch nicht. Oft entsteht der Schaden schon durch den Ausfall des Netzes. Ein DDoS-Angriff kann aber auch als Ablenkungsmanöver genutzt werden, um über einen anderen Weg in fremde Netze einzudringen.
- Welches Interesse könnte an DDoS-Angriffen bestehen?
- Terroristen: *Sabotage an Stromversorgungs- oder Kommunikationsnetzen*
  - Staaten: *Kriegsführung, Spionage und Propaganda („Fake-News“)*
  - Kriminelle: *Schutzgelderpressung („Wenn du bezahlst, wird dein Netz nicht lahmgelegt.“)*  
*oder Vorbereiten weiterer Straftaten durch Eindringen in fremde Systeme*

- **Wir sind auch für das verantwortlich, was wir nicht tun!** Wer sich nicht um die Sicherheit seiner IT-Ausstattung kümmert, schadet potentiell nicht nur sich selbst, sondern auch der Allgemeinheit. Deshalb wurden im IT-Unterricht bereits Maßnahmen in Bezug auf Datenschutz und Datensicherheit besprochen (vgl. Lerninhalte 1.4–05 *Risiken bei der Nutzung digitaler Kommunikationsformen* sowie 1.8–04 *Datensicherheit*). Hier lernst du zunächst weitere Beispiele für Risiken beim Umgang mit Datennetzen kennen. Später werden Maßnahmen zur Konfiguration von Datennetzen besprochen, mit denen die Risiken vermindert werden können.

7. Das Internet der Dinge umfasst keineswegs nur Geräte in Privathaushalten. Durch Fernzugriff lässt sich viel Geld und Energie sparen sowie auch die Lebensumstände von Menschen verbessern, z. B. in der Gesundheitsversorgung. Das betrifft beispielsweise:
- Industrieanlagen
  - Energieversorgungsnetze und auch einzelne Kraftwerke
  - Heizungsanlagen
  - Beleuchtungssteuerung
  - Medizinische Geräte

„Kirchenglocken kann jedermann per Mausklick läuten. Einbrecher kapern Autos, sie knacken Safes mit USB-Sticks; der DSL-Router mutiert zur Angriffswaffe und der Fernseher spioniert bereits ab Werk. Dystopie? Keineswegs! Von der Webcam bis zur Infusionspumpe: Ohne Firmware geht nichts mehr. Mit zunehmender Vernetzung steigen Risiko und Verantwortung.“ (c't 2015, Heft 21, S. 80)

- Beschreibe das grundsätzliche Problem bei der Verwendung vernetzter Geräte.  
*Sicherheitsmaßnahmen, die den Zugriff auf die Geräte verhindern sollen, lassen sich umgehen.*

Auf den folgenden Seiten lernst du ein paar Beispiele dazu genauer kennen.



## 2.5.2 Datennetze II

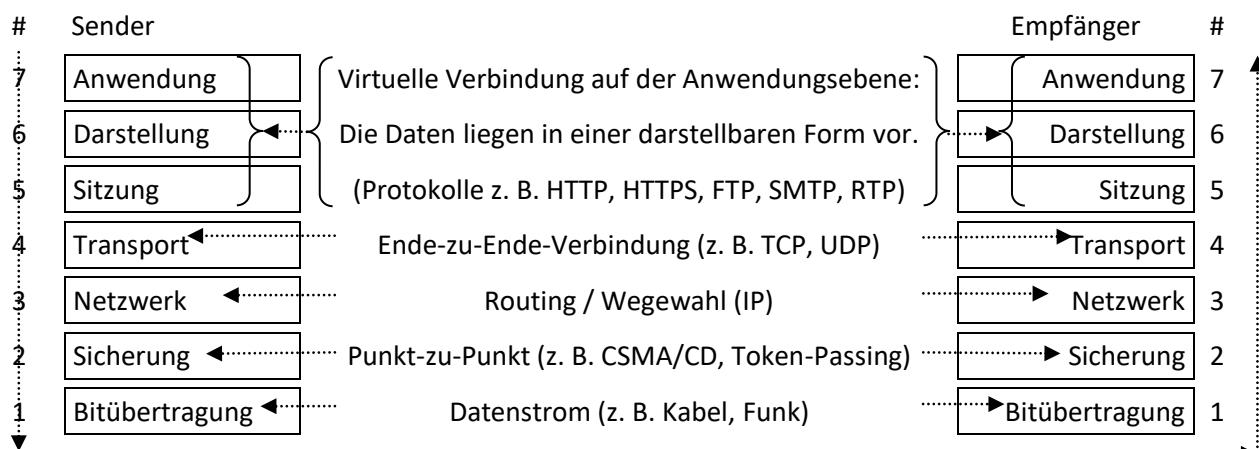
### Ports

8. Angriffsziel Router von Kunden der Telekom:

Ende November 2016 fiel für etwa 900.000 Bundesbürger der Internetzugang und das Telefonnetz aus. Grund war ein Mirai-ähnlicher Wurm, der verschiedene WLAN-Router der Telekom über eine Sicherheitslücke lahmlegte. Die Lücke war der TCP-Port 7547, der es ermöglichte, bei den Routern anzuklopfen, um z. B. ein Softwareupdate zu veranlassen.

Du kennst die Darstellung des OSI-Modells bereits aus dem vorigen Arbeitsblatt:

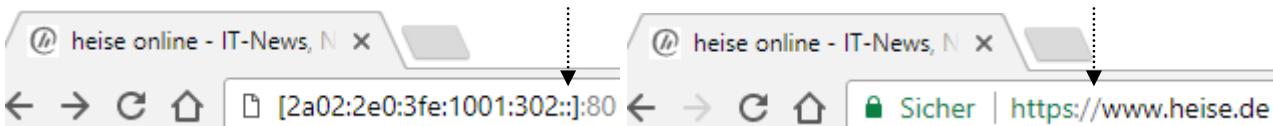
- Auf der OSI-Schicht 4 wird der Transport von Daten gewährleistet.
- Für die Anwendungsebene muss aber darüber hinaus bekanntgegeben werden, wie mit diesen Daten umzugehen ist – also welches Protokoll verwendet wird.



- Die Information, welches Protokoll auf der Anwendungsebene zu verwenden ist, wird mit einer **Portnummer** im Zusammenhang mit der IP-Adresse übermittelt:

Der **Port** ist dem TCP-Protokoll zuzuordnen, also der Schicht 4 des OSI-Modells. Die Portnummer wird mit einem Doppelpunkt abgetrennt an die IP-Adresse angehängt.

Eine IP-Adresse (IPv6) könnte vollständig z. B. so aussehen und zu dem Internetauftritt rechts führen:



Es gibt Standardports für unterschiedliche Protokolle, z. B. für **FTP** ist der Standardport **21**.

Die meisten FTP-Zugriffe sind passwortgeschützt.

Für diese Anwendung ist ein FTP-Client erforderlich.

Die Oberfläche sieht ähnlich aus wie im lokalen Dateisystem – mit dem Unterschied, dass die Dateien hier auf einem entfernten Rechner liegen und über das Internet zugegriffen wird.

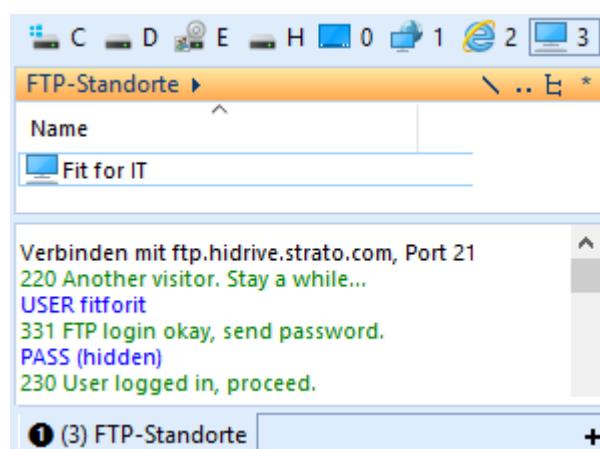
Weitere Beispiele für Standardports:

**25: SMTP** (E-Mail-Versand)

**80: HTTP** (Webserver)

**110: POP3** (Client-Zugriff auf E-Mail-Server)

**443 HTTPS** (sicherer Webserver)



- Ein Angriffsziel ist das Port-Forwarding: Für Geräte, die von außen erreichbar sein müssen, werden am Router Port-Weiterleitungen eingerichtet. Dabei leitet der Router Datenpakete, die über einen bestimmten Port eintreffen, an ein zuvor festgelegtes Gerät im Lokalen Netz weiter.



## 2.5.2 Datennetze II

### WLAN-Router

9. WLAN-Router lassen sich teilweise mit einfachen Mitteln attackieren. Das kann hier anhand eines Beispieldes wird nachvollzogen werden. Eventuell ist an der Schule auch ein „Spielrouter“ verfügbar:
- Wenn man, wie auch von Servicetechnikern empfohlen, den WPA2-Schlüssel nicht ändert, kann der ab Werk eingestellte Schlüssel oft berechnet werden, weil die Algorithmen dafür bekannt sind oder sich herausfinden lassen. Man benötigt lediglich die MAC-Adresse.

Erster Schritt: Die IP-Adresse des Routers ermitteln.

Wenn man die IP-Adresse schon kennt, weil sie auf der Einstellung ab Werk belassen wurde, kann man sich diesen Schritt sparen.

Zweiter Schritt: Die MAC-Adresse wird mit dem Kommando arp ... zurückgegeben.

```
Eingabeaufforderung
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

C:\>nslookup fritz.box
Server: fritz.box
Address: fd00::3a10:d5ff:fe55:6b9c

Name: fritz.box
Addresses: fd00::3a10:d5ff:fe55:6b9c
          192.168.201.11

C:\>arp -a 192.168.201.11
Schnittstelle: 192.168.201.20 --- 0x3
      Internetadresse          Physische Adresse      Typ
      192.168.201.11           38-10-d5-55-6b-9c  dynamisch
```

- WLAN-Router werden tatsächlich manchmal mit der Kombination Benutzername „admin“ und Kennwort „admin“ ausgeliefert! Wenn hier der Benutzer nichts geändert hat, kann der Router leicht übernommen werden. Ansonsten gibt es Tools zu kaufen, die das Kennwort knacken. Man kann beispielsweise den Datenverkehr in einem lokalen Netz belauschen und Datenpakete gezielt abfangen – auch verschlüsselte HTTPS-Verbindungen. Damit lassen sich Benutzernamen und Passwörter ermitteln, aber auch VoIP-Gespräche belauschen.
- Was dann? – Beispielsweise kann ein Krimineller einen anderen DNS-Server eintragen:

Übersicht  
Internet  
Online-Monitor  
**Zugangsdaten**  
Filter  
Freigaben  
MyFRITZ!  
Heimnetz  
WLAN  
Diagnose  
System

Zugangsdaten

Internetzugang IPv6 LISP DNS-Server

Geben Sie an, ob für die Namenauflösung die vom Internetanbieter zugewiesenen oder andere DNS-Server genutzt werden sollen.

DNSv4-Server

Vom Internetanbieter zugewiesene DNSv4-Server verwenden (empfohlen)  
 Andere DNSv4-Server verwenden  
Bevorzugter DNSv4-Server: 104 . 76 . 34 . 109  
Alternativer DNSv4-Server: 104 . 76 . 133 . 38

DNSv6-Server

Vom Internetanbieter zugewiesene DNSv6-Server verwenden (empfohlen)  
 Andere DNSv6-Server verwenden  
Bevorzugter DNSv6-Server:  
Alternativer DNSv6-Server:

Übernehmen Abbrechen

Danach hat der Angreifer leichtes Spiel: Nach Eingabe einer Internetadresse wird die IP-Adresse eines gefälschten Internetauftritts auf einem anderen Server aufgerufen. Der Benutzer bemerkt davon nichts.