



## **„Digitale Selbstverteidigung in der Familie“**

Andrea 'Princess' Wardzichowski

Chaos Computer Club Stuttgart e.V.

<http://www.cccs.de/>

[princess@bofh.de](mailto:princess@bofh.de)

PH Ludwigsburg, VL Gesine Kulcke, 15.5.2017

Der heutige Vortrag soll beleuchten, wie man sich und seine/di einem anvertrauten Kinder sicher(er) durch die digitale Zeit bringt und sie an die Möglichkeiten, aber auch Problematiken heranzuführt.

# Über den CCCS / über mich

Über den CCCS:

Seit Sommer 2001 Treffen  
Seit Oktober 2003 monatliche Vortragsreihe  
**Spaß am Gerät, aber auch Gefahren beim  
bedenkenlosen Einsatz von Technik**

Über mich:

Seit November 1990 im Netz aktiv  
(Mail, News, IRC, Relay Parties, CCC)  
Heute: CCCS e.V. (Presse), Haecksen,  
querulantin.de

In vielen großen und inzwischen auch in vielen kleinen Städten gibt es sog. Chaostreffs, die im Sinne des CCC e.V. agieren, der 1986 in Hamburg gegründet wurde.

Ich selber bin auch schon sehr lange im Netz unterwegs und habe meine Homepage aufgebaut, damit man meine aktuellen Veröffentlichungen und Vorträge eher findet, als meine Jugendsünden aus Usenet-Zeiten.

Aufgrund meiner langjährigen Erfahrung versuche ich, Handlungsempfehlungen für die Internetnutzung abzuleiten, die mir sinnvoll erscheinen.

Es wird heute viele Beispiele aus dem „richtigen Leben“ geben und wir befinden uns GENAU in dem Spannungsfeld zwischen „Spaß am Gerät“ und der Technikfolgenabschätzung.

# Agenda

- Vorwort
- Was kann das Internet?
- Datenschutzgesetz und Privatsphäre
- Rechtliche Implikationen
- Wo sind meine Daten einigermaßen sicher?
- Wie kann ich mich und meine Familie schützen?
- Auswirkungen

Es soll aufgezeigt werden, wo die Gefahren lauern, aber es sollen auch Lösungen und Auswege gezeigt werden, denn eines ist sicher: die Digitalisierung läßt sich nicht zurückdrehen.

# Vorwort

- Erziehung erfolgt nicht nur durch **Anweisungen**, sondern auch durch **Nachahmen**
- Um Kindern also einen angemessenen Umgang mit Medien zu vermitteln, ist es unerlässlich, die Eltern ins Boot zu holen.

**=> Aber das wissen Sie schon!**

**=> Leider sind Eltern (datenschutz-)technisch eher unbedarf**

**=> Was können wir dennoch tun?**

Eigentlich ist jeder, der nicht „von Hause aus“ Jurist oder eben ITler ist, unbedarf, was Datenverarbeitung, Datensicherheit und Datenschutz angeht. Das ist auch nicht verwerflich, schließlich kann man nicht Experte auf jedem Gebiet des täglichen Lebens sein. Allerdings hat die Digitalisierung der Gesellschaft Auswirkungen, derer man sich bewußt werden muss: oft denkt man bei den Konsequenzen einfach nicht weit genug.

Zusammenarbeit: es nützt kaum etwas, wenn eine Familie keine Bilder von sich ins Netz lädt, wenn dies beim Kindergeburtstag oder im Sportverein dann unterlaufen wird. Daher ist die Absprache und das Überzeugen vieler Eltern so wichtig.

## Wie unterscheidet sich das Internet von anderen Medien?

- **Zeitung** (redaktionell kontrolliert)
  - Leider kaum Inhalt für KiTa-Kinder.
- **Radio** (redaktionell kontrolliert)
  - Weitestgehend harmlos (habe ich auch morgens gehört als Schülerin)
- **Fernsehen** (redaktionell kontrolliert)
  - Welche Sendungen? Wie lange?  
=> **Heutzutage kommen Krimis, die früher um 21:45 liefen, den ganzen Tag über!**
- **Internet (inhaltlich unkontrolliert)**
  - **Es gibt im Internet nichts, was es nicht auch in der wirklichen Welt gibt, aber es ist NICHT alles kindgerecht**
  - **Privateste Daten können hineingelangen (und nie wieder heraus)**

Betrachten wir einmal verschiedene Medien, so fällt auf, dass „herkömmliche“ Medien wie Zeitung, Rundfunk und Fernsehen doch mindestens einer redaktionellen Kontrolle unterliegen.

Dies trifft für weite Teile des Internets NICHT zu.

Aber auch bei den herkömmlichen Medien: kaum jemand ließe Grundschüler stundenlang und hemmungslos durch alle Kanäle zappen! Es gibt auch dort viele Sendungen, die zwar nachmittags laufen, nicht aber kindgerecht sind. Z.B. werden Krimis, die früher um 21:45 Uhr liefen, heute auf Spartensendern tagsüber wiederholt.

Fazit: unbeaufsichtigter Internetkonsum frühestens ab dem Teenie-Alter. Dies bedeutet auch: vorher kein Smartphone. Gerade hier müssen sich dann aber die Mehrheit der Eltern in der Klasse einig sein! Sonst geht's gleich los mit der Diskriminierung.

# Was kann das Internet?

- Wissensbasis und Datenquelle
- Davor: was es in der Bibliothek nicht gibt, ist faktisch unerreichbar an Wissen

## **Heute gefragte Kernkompetenzen:**

- Gut suchen können (nicht erschlagen werden von den Ergebnissen)
- Quellen bewerten (echt oder fake news?)

Leider wird das Netz als Wissensbasis viel zu wenig genutzt. Man kann sich heute viel besser über Studiengänge und Ausbildungen informieren, aber mein Eindruck ist, dass diese Chance vertan wird. Nach wie vor scheinen z.B. Realschüler je nach Geschlecht nur die drei gleichen Berufe zu kennen wie noch vor 10 oder 20 Jahren.

Bereits im Geschichtsunterricht lernte ich, wie Quellen einzuordnen und zu bewerten sind. Dies ist heute wichtige denn je!

Beispiel: zu welchem Zeitpunkt erscheint eine Seite mit Infos? War sie schon länger da (und wird auch in Archiv-Suchmaschinen gefunden) oder sprießt sie aus aktuellem Anlaß aus dem Boden?

„Der Stuttgarter Bahnhofsturm steht auf Holzpfehlern und die werden wegbrechen wenn das Grundwasser abgesenkt wird.“

Stand so im Internet! Allerdings erst, als die Diskussion darum begann. Es ist also kaum als Bau-Dokumentation zu werten oder als Beweis für das verwendete Material.

# Datenschutzgesetz und Privatsphäre

- Personenbezogene Daten / Privatsphäre  
=> Kinder sollten lernen, was personenbezogene Daten sind und wen diese etwas angehen
- **Datenschutzgesetz**
  - Zweckgebundenheit
  - Datensparsamkeit  
=> dies schützt vor verarbeitenden Stellen, nicht aber die Informationen die wir/Kinder **selber hochladen und veröffentlichen**
- „nix zu verbergen“? Doch. Eine Menge.

Ein besonderes Augenmerk muß man nicht nur im Internet auf seine privaten/personenbezogenen Daten haben. In einem normalen Leben werden die Daten mindestens beim Einwohnermeldeamt (Meldegesetz), bei der Bank (Gehaltskonto) und bei einem Telekommunikationsanbieter (Festnetz, Mobil) gespeichert. Füge ich nun noch selber Informationen im Netz hinzu, muß ich wissen, was mit diesen passieren kann.

In Deutschland gilt das Datenschutzgesetz. Dies greift aber nur für Daten, die andere Stellen über mich speichern. Stelle ich selber Informationen ins Netz, können diese ge- und mißbraucht werden.

Schon viele Erwachsene können nicht überschauen, was ihre Äußerungen im Netz bewirken können, geschweige denn können dies Heranwachsende. Ziel ist, ein Bewußtsein für Privatsphäre und Privates zu schaffen. Beispiel Twitter: das will doch nach ner Weile echt keiner Wissen was mir wann durch den Kopf geschossen ist und was ich wann gemacht habe.....

Auch Erwachsene haben häufig kein Gefühl dafür, daß sie durchaus IMMER etwas zu verbergen haben. Dazu gehören z.B. Einkommensverhältnisse und Krankheiten.

Lebenssituationen können sich ändern: grad letzte Woche: früher Hobbyhure, nun AfD Politikerin! Das Netz aber vergisst nicht

# Warum Privatsphäre schützen?

- Niemand weiß, was zukünftig mit öffentlich zugänglichen Daten passiert
  - Künftige Arbeitgeber, künftige Partner
- Bilder
  - Gesichtserkennung wird wieder an Bahnhöfen getestet
  - Private Firmen greifen auf öffentliches Material (facebook) zu
  - Kinder sind bei ihren Sportvereinen prima auflauerbar.

Eltern finden es sicher „ganz süß“, wenn die Familie oder auch die halbe Welt sich an ihren Kinderbildern entzückt. Aber: Kinder werden auch mal erwachsen und wollen sich nicht, daß jeder potentielle Arbeitgeber oder auch Partner (!) alle peinlichen Kinderfotos kennt. Daran sollte man denken, solange man für seine Kinder entscheiden darf und muss.

Eine Freundin fragte mich kürzlich, warum es denn „schlimm“ sei, wenn man mit Bild und Namen im Internet stünde. Es ist nicht „schlimm“ in dem Sinne, aber ich möchte gern selber entscheiden, wem ich meinen Namen sage. Schließlich laufe ich doch auch nicht jeden Tag mit einem Plakat herum, auf dem groß mein Name steht, damit jeder auf der Straße und in der Stadtbahn ihn sehen kann. Und: selbst wenn die Bilder gelöscht sind wo sie waren: aus den Archiven und Suchmaschinen-Caches sind sie noch lange nicht!

Ich möchte auch nicht, daß pausenlos Kameras aufzeichnen, wann ich wo gewesen bin. Allerdings sehe ich auch die Unschuldsvermutung langsam aber sicher schwinden: wird es in naher Zukunft so sein, daß ICH nachweisen mss (durch Kartentransaktionen oder eben Video) daß ich NICHT am Schauplatz eines Verbrechens war?

# Daten aus der Hand geben?

- Nutzungsbedingungen von facebook
- Dito whatsapp
- Dito Partnerbörsen (!)
- Lustig auch: **Linkedin** fragt nach dem Mailpasswort (!), damit es das Adressbuch herunterladen kann und alle einladen.
- „There is no cloud, just other people's computers“

Daten, die man aus der Hand gibt, entziehen sich der eigenen Kontrolle. Sie können auch mißbraucht werden.

Oft erscheint einem das ob der eigenen Unwichtigkeit nicht so relevant, aber häufig werden Daten durch bestimmte Umstände zusammengeführt und ergeben ein vorher nicht dagewesenes Bild.

Beispiel: der Chef bekommt mit, wieviel Zeit ein/e Angestellte/r auf facebook oder mit whatsapp verbringt.

Beispiel Linkedin: auch hier kann niemand verklagt werden, schließlich hat man sein Passwort SELBER an Dritte herausgegeben.

# Rechtliche Implikationen

- **Wichtig: alle Gesetze gelten auch online!**
  - z.B.: Beleidigung (per SMS, Whatsapp...)
  - z.B.: Urheberrecht  
(Musik/Filme aus illegalen Quellen laden)
  - z.B. **Fotos ungefragt machen und Hochladen:**  
**Par. 33 (22+23) KunstUrhG** bis 1 Jahr Freiheitsstrafe oder Geldstrafe  
Par. 201A StGB: bis 1 Jahr Freiheitsstrafe oder Geldstrafe  
(„Spannerparagraf“)
- => Anschlußinhaber ist zeitnah auch ohne Vorratsdatenspeicherung zu ermitteln

## Par. 201A StGB

Am 6. August 2004 trat § 201a Strafgesetzbuch (StGB) („Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen“) in Kraft[28], der unter bestimmten Umständen schon für das bloße Erstellen eine Strafbarkeit vorsieht. Danach wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer

(1) von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt.

(2) Ebenso wird bestraft, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht.

(3) Wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

# Rechtliche Implikationen

- **Wichtig: alle Gesetze gelten auch online!**
  - z.B.: Beleidigung (per SMS, Whatsapp...)
  - z.B.: Urheberrecht  
(Musik/Filme aus illegalen Quellen laden)
  - z.B. **Fotos ungefragt machen und Hochladen:**  
**Par. 33 (22+23) KunstUrhG** bis 1 Jahr Freiheitsstrafe oder Geldstrafe  
Par. 201A StGB: bis 1 Jahr Freiheitsstrafe oder Geldstrafe  
(„Spannerparagraf“)
- => Anschlußinhaber ist zeitnah auch ohne Vorratsdatenspeicherung zu ermitteln

## Par. 33 KunsturhG

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen den §§ 22, 23 ein Bildnis verbreitet oder öffentlich zur Schau stellt.

(2) Die Tat wird nur auf Antrag verfolgt.

## Par. 22

Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, daß er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

## Par. 23

(Zeitgeschichte, Beiwerk bei Landschaft, Versammlungen, ..)

## Wo sind meine Daten einigermaßen sicher?

- 100% Sicherheit gibt es nirgends
- Grundsätzlich: bei Anbietern auf deutschen Boden gilt das Datenschutzgesetz und der Rechtsweg ist einfacher
- Mail: **posteo.de**, GMX, web.de, mehrere Mailadresse für privat/Bestellungen
- Internetprovider in Deutschland für Webseiten
- Cloud: owncloud, nextcloud selbst betreiben  
**ABER:** Sicherheitspatches regelmäßig einspielen!

Gegen staatliche Überwachung (die in den letzten Jahren immer weiter ausgedehnt wird), kann man natürlich wenig machen, außer rechtzeitig protestieren.

Beispiel: Einführung des RFID Passes nach dem 11.9.2001. Dieser hätte die Anschläge zu keinem Zeitpunkt verhindert.

Dito: Vorratsdatenspeicherung. Speichern von Daten beim Provider für 14 Tage wäre völlig ausreichend („Quick Freeze“), da bei schweren Straftaten idR. schnell ermittelt wird. Urheberrecht hingegen verletzt nicht Leib und Leben, sondern nur den Stolz der Rechtheverwerter.

## Wie kann ich mich und meine Familie schützen?

- Datensparsamkeit bei Adresse, Telefonnummer, Bildern, Veröffentlichungen (z.B. Twitter)
- Vorhandene Sicherheitsmechanismen nutzen (Nutzerkreis einschränken, nicht jeden zum „Freund“ machen, hilft aber auch nicht bei Programmierfehlern seitens der Betreiber)
- Messenger: **signal** statt whatsapp
- Ideal: Mails verschlüsseln

**=> leider gibt es Sicherheit nur mit etwas Aufwand  
=> man muss Freunde und andere Eltern  
„mitnehmen“**

Im IT-/Internetbereich ist es wie im richtigen Leben: Sicherheit bedeutet Aufwand.

Allerdings: es jammert eigentlich auch niemand, daß er beim Verlassen der Wohnung die Tür abschließen sollte und vielleicht im Erdgeschoß alle Fenster schließen. Auf diesem Gebiet hat sich – zumindest in der Stadt – das Bewußtsein für Sicherheit als „normal“ eingebürgert. Für die digitale Welt muß das noch geschehen.

Auch: Bildersammlungen für Großeltern mit Passwort schützen, damit die Bilder nicht bei google landen.

# „Sicherer Surfen“

- **Privates Browserfenster** nutzen  
(firefox, opera)
- **Cookies** bei Beenden des Browsers löschen
- **Alternativen** zu google als Suchmaschine:  
startpage.com, duckduckgo.com, bing.com
- **Komplett anonym surfen: tor-browser**  
<https://www.torproject.org/>  
(das sog. „dark web“ ist nur über diesen zugänglich. Aber tor hilft Menschen in Ländern, in denen freie Meinungsäußerung nicht möglich ist, zu kommunizieren!)
- Keine Passworte im Browser abspeichern
- Sichere Passworte wählen anhand Lieblingslied oder -gedicht

Ausführlich: auf den Cryptoparties des CCCS in der Stadtbibliothek am Mailänder Platz.

## Auswirkungen: Mobbing, Sucht, Regeln

**Mobbing** (kein Gefühl dafür, andere zu verletzen, weil das Medium die Konfrontation verhindert) => „**Sage nichts, was Du nicht auch jemandem ins Gesicht sagen würdest**“

- **Sucht** auch bei Erwachsenen erkennbar
- **Regeln** wie „Verkehrsregeln“, nicht wie Verbote
- Gefühlte **Nähe** (Chatpartner sind keine Fremden!)
- **Vorbild sein** (es ist schwer, in der Materie zu sein!)

**NETiquette: „Vergiß nie, daß am anderen Ende der Leitung auch ein Mensch sitzt“.** Zusammen mit „Sage nichts, was Du nicht auch jedem ins Gesicht sagen würdest“ ist man schon ziemlich auf der sicheren Seite. **In der Realität aber sind auch Erwachsene feige:** es ist viel leichter, sich bei Hausverwaltung oder Vermieter zu beschweren, statt direkt zum Nachbarn zu gehen und ihn zu bitten, die Musik leiser zu machen oder nicht in der Mittagspause zu hämmern.

**Suchtgefahr** besteht auch bei Kindern, die viel Sport machen und draußen sind: das „Gedaddel“ ist einfach attraktiv.

Zu **Chatpartnern** wird durch regelmäßige Kommunikation eine Beziehung aufgebaut. **Tip:** Mailadresse mit anderem Namen anlegen und sich mal irgendwo anmelden und 14 Tage lang jeden Tag eine Stunde chatten/dort verbringen. Männer melden sich testweise als Frauen an und lernen freundschaften.

Preisgabe von Hobbies und Aufenthaltsorten führt nicht nur dazu, daß **Eltern** wissen wo ihr Kind ist! Andere wissen das dann auch (whatsapp, facebook).

# Termine

- 19.-21.5.2017  
no-spy-Konferenz  
<https://no-spy.org/>  
Literaturhaus Stuttgart
- Cryptoparty  
Mails verschlüsseln, sicherer Surfen,  
Smartphone sicherer einstellen  
Bibliothek am Mailänder Platz  
Eintritt frei!

# Fragen und Diskussion



?

?

?

Veranstaltungen: 2. Donnerstag im Monat Vortrag in der Stadtbibliothek,

Cryptoparties ca. einmal im Quartal, auch Stadtbibliothek.

Ebenso: Reihe „Meine Daten“