Medienkompetenz Basiswissen „digitale Medien“

Wichtige Grundlagen, die Viele „*wissen*“,
die aber nur Wenigen *bewusst* sind

Bewusstheit für:

1. Das Sicherheitsgefühl trügt durch den sicheren realen Ort („vertraut“, „nah“), an dem sich die Person befindet und evtl. einen absolut unsicheren virtuellen Ort öffnet. Dieser hat jedoch reale Auswirkungen.

2. Das Meiste wird heute über Software realisiert. So hat die Mehrzahl der heute verkauften elektronischen Geräte keine echten, direkt real wirksamen Schalter mehr. Auch „Regler“ (z.B. „Lautstärke“) und „Anzeigen“ (z.B. „Akkuladung“) sind nicht mehr direkt an die Realität gekoppelt. => „Alles Schein“ => „Alles Interpretation“ => Alles mehr oder weniger menschlicher „Schummel“.

3. Digitale Daten (e-mails, Instagram-Bilder, …) können jederzeit, lautlos, verlustfrei und nahezu unendlich oft kopiert, gespeichert und weitergeleitet werden.

4. Digitale Daten (e-mails, SMS, …) können (nahezu?) unbemerkt gefälscht, verändert bzw. manipuliert werden. („Social Engineering“, „Identitätsmissbrauch“)

5. Die Kommunikation kann auch unbemerkt beginnen, sobald eine Netzwerkverbindung besteht (WLAN oder „mobile Daten“ aktiviert, Netzwerkkabel eingesteckt, NFC Ausweis in der Nähe eines Lesegerätes, …)

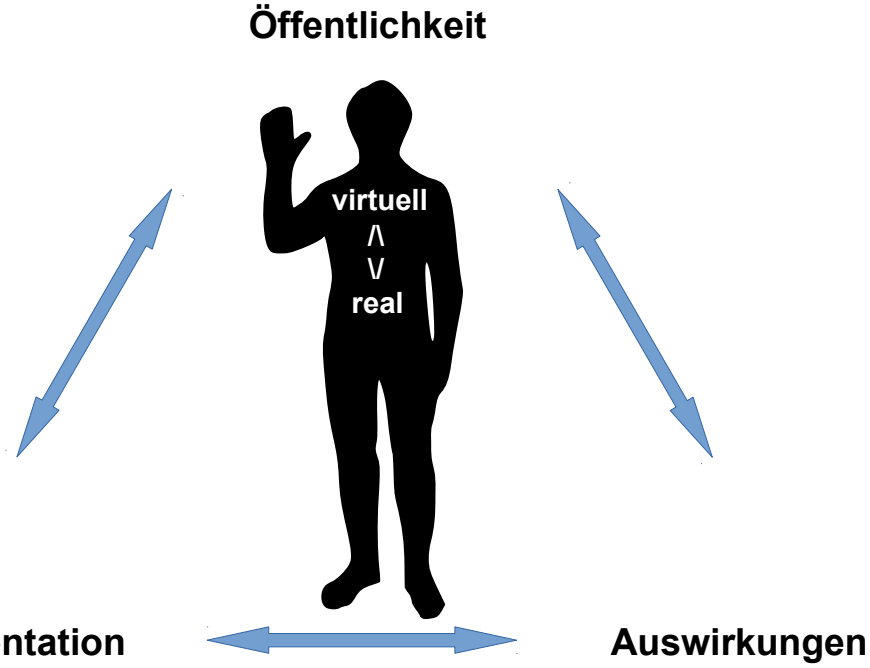
6. Das Internet ist ein Netz! Jede Kommunikation über das Internet läuft über mehrere (unbekannte) „Knoten“. Dabei lässt sich nicht mit Sicherheit sagen, wer an welchem Knoten Alles unbemerkt lesen, auswerten, verändern und kopieren kann. Jede zusätzliche Kommunikation und jeder zusätzliche Knoten vervielfacht die Unsicherheit.

7. „Freundschaft“ bedeutet auch, Verantwortung dafür zu übernehmen, dass mein Handeln dem Anderen* nicht schadet.

8. Naivität macht Kriminalität erst lohnend.

=> Digitale Kommunikation ist keine „reale“ Kommunikation. Sie verlangt einen umsichtigeren Umgang und sorgfältige Datensparsamkeit. Merkwürdigkeiten sind unbedingt in der realen Welt direkt von Mensch zu Mensch klären. Dabei ist dem bekannten Menschen in der realen Begegnung grundsätzlich mehr zu glauben, als „der Technik“ (= „dumme“ Software von „fremden Menschen“).

1. Sicherheitsgefühl



Was gibt uns Sicherheit? *Ziel: Schaden für sich und Andere vermeiden!*
Reale Wahrscheinlichkeitsrechnung <=> persönliche Abschätzung

Sicher sein? Wovor?
Sicher vor Rufschädigung sowie körperlichem oder finanziellem Schaden ...
Sicher vor Einbrechern, Verbrechern, Erpressern, Kinderschändern, sexueller Belästigung, ...
Sicher, dass das, was in der Zeitung / in einem Buch steht, in den Nachrichten kommt, … stimmt.
Sicher, dass die Informationen nicht manipuliert sind, bzw. mich manipulieren wollen.
„Stimmt das?“ „Ja sicher!“
Wissen <=> Glauben, Glaubwürdigkeit
Sicher, nicht überwacht, ausspioniert, registriert, aktenkundig zu werden.
Sicher, unbeschadet seine Meinung frei äußern zu können.
Sicher, dass „Vertrauliches“ vertraulich bleibt.

Sicher fühlen? Wovor? Wann fühlen Sie sich wohl?

Sicherheitsgefühl:
Psychologisch: Mensch benutzt die Technik im „sicheren“ zu Hause bzw. ganz nah bei sich.

Zu Hause	<=>	**Weltöffentlich**
Real? Gefühlt?		Virtuell? Bewusst? (Bsp. fremder Marktplatz)
Vertraut, geborgen, locker, „sicher“		Vorsichtig, zurückhaltend, überlegt, umsichtig
Hohe Kontrolle		Wenig Kontrolle, „machtlos“
Wenig Kontakt		Viele Kontakte
Bsp: Verein, Bäcker, Friseur		Bsp: twitter, facebook, e-mail, WhatsApp, chat

Sicherheit mit den Medien widerspricht weitgehend dem Sicherheits**gefühl** => Verstand / Bewusstheit

Höchste Sicherheit (unpraktisch)	**Höchste Bequemlichkeit (unsicher)**
(Paranoid)	(Naiv)
Tresortür	Zugangsloch (Sommer: offene Fenster u Glastüren)
Mauer	Offen
Keine Verbindung nach Außen	Laut schreiend Jeden einladen

Beispiel für die Verdeutlichung:

Male Deine ideale Wohnung. Anschließend: Wovon lebst Du? Wann bist Du dort? Wie ist es im Winter? Wie im Sommer? Was ist mit Diebstahl, Erpressung oder Mobbing? Stell Dir vor, es ziehen sehr viele, sehr fremde Leute in die Gegend. Manche sind neidisch, manche suchen das schnelle Geld, manche brauchen eine Tarnadresse für ihren Drogenhandel, manche haben Spaß daran, andere zu ärgern. Stell Dir die Situation bildlich vor. Wie sieht Deine ideale Wohnung dann aus? Wie fühlst Du Dich wenn Du nackt die Wohnung verlassen musst? Drückst Du zusätzlich jeder Person auf dem Weg ein Nacktbild von Dir in die Hand? Genau da befindet sich Dein Smartphone und genau diese Situation ist heute im Internet, wenn Du Snapchat, Instagram, WhatsApp, facebook, e-mail, Google, iCloud, Dropbox, Instagram oder … benutzt.

2. Alles ist Software (= von fremden Menschen geregelt)

Das Meiste wird heute über Software realisiert. So hat die Mehrzahl der heute verkauften elektronischen Geräte keine echten, direkt real wirksamen Schalter mehr. Auch „Regler“ (z.B. „Lautstärke“) und „Anzeigen“ (z.B. „Akkuladung“) sind nicht mehr direkt an die Realität gekoppelt. => „Alles Schein“ => „Alles Interpretation“ => Alles mehr oder weniger menschlicher „Schummel“.

Beispiel für die Verdeutlichung:

Bastelprojekte mit der Verbindung von Hardware und Software - die auch mal gezielt „schummeln“ - bieten sich an (z.B. auf der Grundlage von RaRoPhoPl). Oder kleine Software Projekte, die bewusst falsche Tatsachen vorspiegeln oder das eigene technische Gerät anders „reagieren“ lassen, als erwartet. So lässt sich z.B. ein kleines Programm erstellen, das nach Betätigung des „Ein-Aus-Knopfs“ das Ausschalten des Gerätes vorspielt in Wirklichkeit aber das Mikrofon aktiviert und alles aufnimmt. Auch ein dazugehöriger „Einschaltvorgang“ kann entsprechend simuliert werden.

3. Alles doppelt, auch das Doppelte

Digitale Daten (e-mails, Instagram-Bilder, …) können jederzeit, lautlos, verlustfrei und nahezu unendlich oft kopiert, gespeichert und weitergeleitet werden.

Beispiele für die Verdeutlichung:

Anfertigung von Bildschirmfotos von Smartphone-Apps mit privaten Bildern oder Texten (auch solchen, die sich angeblich selbst löschen, oder „verschlüsselt“ übertragen wurden). Ebenso am Computer. Evtl. mit einer externen Kamera. „Flüsterpost“ am Beispiel eines harmlosen Bildes: Wie lange dauert es, bis dieses bei allen in der Gruppe / im Kurs / in der Klasse (unverändert, aber auch evtl. absichtlich verändert) angekommen ist? Auch direkt real mit identischen Postkarten die durch viel Hände laufen...

4. Unglaubwürdig?

Digitale Daten (e-mails, SMS, …) können (nahezu?) unbemerkt gefälscht, verändert bzw. manipuliert werden. („Social Engineering“, „Identitätsmissbrauch“)

Beispiele für die Verdeutlichung:

Wir verschicken eine glaubwürdige e-mail oder Freundschaftsanfrage auf facebook im Namen eines Anderen. Wir „machen“ glaubwürdig per SMS im Namen eines Anderen „Schluss“.

Oder arbeiten geschickt mit GIMP im Rahmen eines Fotoprojekts und dichten jemandem den Aufenthalt an einem anderen Ort an.

5. Ich mach doch gar nichts...

Die Kommunikation kann auch unbemerkt beginnen, sobald eine Netzwerkverbindung besteht (WLAN oder „mobile Daten“ aktiviert, Netzwerkkabel eingesteckt, NFC Ausweis in der Nähe eines Lesegerätes, …)

Beispiele für die Verdeutlichung:

- Wir stellen ein freies WLAN unter dem Namen „Telekom“ zur Verfügung und schauen, welche Geräte sich arglos damit verbinden.

- Wir aktivieren NFC am Smartphone und testen mit diesem, in welchen Taschen sich NFC-Karten (wie z.B. Personalausweise) befinden.

6. „net“ heißt „Netz“ und nicht „*direkte Schnur*“

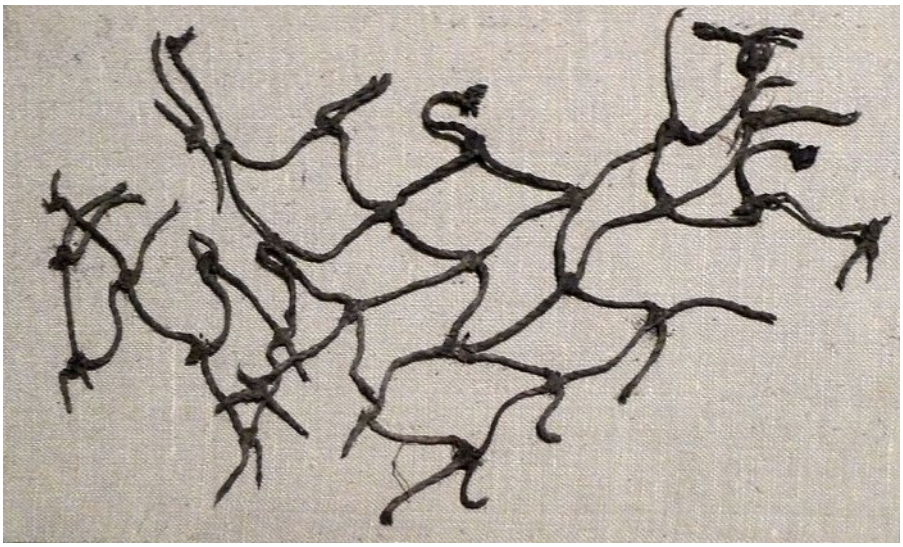


Abbildung 1: File source: http://commons.wikimedia.org/wiki/File:HMB_Fischernetz_Jungsteinzeit.jpg

Das Internet ist ein Netz! Jede Kommunikation über das Internet läuft über mehrere (unbekannte) „Knoten“. Dabei lässt sich nicht mit Sicherheit sagen, wer an welchem Knoten Alles unbemerkt lesen, auswerten, verändern und kopieren kann. Jede zusätzliche Kommunikation und jeder zusätzliche Knoten vervielfacht die Unsicherheit.

Beispiele für die Verdeutlichung:

Wie werden Anfragen im Internet verarbeitet (DNS, ...) und weitergeleitet? Wie werden Nachrichten verschickt? Wo befinden sich Bilder die ich sehe? Wo befinden sich Bilder, die ich mit dem Smartphone anfertige? Wo evtl. noch? Und wenn ich diese digital verschicke? Wer hat wie, welchen Zugriff auf was? Wem kann ich vertrauen? (=> real bekannten Menschen in der realen Welt) Und was nicht? (=> allem, was auf Software beruht)
=> Ein real ausgedrucktes Foto, das ich jemandem direkt zeige, kann ein Vertrauensbeweis sein. Ein digital verschicktes Foto hingegen kann „Vertrauen“ gegenüber unzähligen, wildfremden Personen bedeuten. Auf jeden Fall gilt, wer digitale Fotos als „Vertrauensbeweis“ fordert, ist so „naiv“ (oder „dumm“? oder „bösartig“?), dass er das Vertrauen definitiv nicht verdient hat.

Real:

Ein Schallrohr bzw. ein Dosen-Schnur-Telefon überträgt die Nachrichten direkt. Wie sieht im Gegensatz dazu ein Netz bzw. das Internet aus? Wir simulieren das Gleiche mit einem Wasserschlauch und im Gegensatz dazu mit einem komplexen Rohr-Verteilungssystem mit diversen Abzweigungen und zusätzlichen Wasserhähnen.

7. Freundschaft heißt Verantwortung

„Freundschaft“ bedeutet auch Verantwortung dafür zu übernehmen, dass mein Handeln dem Anderen* nicht schadet. Jetzt **und in der Zukunft**. Die Auswirkungen eines „Scherzes“ können heute viel weitreichender (sowohl räumlich als auch zeitlich) sein, als vor der Digitalisierung. Auf eine „Pädagogik im Atomzeitalter“ müsste so schon lange eine „Pädagogik im Digitalzeitalter“ aufbauen.
Die Komplexität menschlicher Individualität mit jeweils eigenen individuellen Vorlieben, Sichtweisen, ... und sozialen Beziehungen, kann bereits heute technisch weitgehend erfasst und genutzt werden („Big Data“). Eine „Rasterfahndung“ bis zum einzelnen Individuum, unabhängig von deren zugewiesenen Gruppeneigenschaften oder irrelevanten Äußerlichkeiten, ist technisch relativ unproblematisch. Diese Individualisierung der Daten bis auf Personenebene - mit einem Fokus auf jedes Individuum - hat bei den IT-Konzernen (Google, facebook, Microsoft, …) längst begonnen. Die auf den einzelnen Menschen ausgerichtete Computerwelt ist damit bereits weiter als die „Gesellschaft“, die immer noch nach groben äußerlichen Zwangsgruppen (z.B. „Männer und Frauen“ oder „Schwabe“) einteilt. Dabei versuchen Menschen sich die Welt zu vereinfachen, können den Individuen aber nie wirklich gerecht werden.
Die IT-Konzerne hingegen freuen sich über jede individuelle Eigenheit die sie erfahren können...

Beispiele für die Verdeutlichung:

Wenn ich kein Problem mit Nacktbildern von mir habe, heißt das nicht, dass damit Andere auch kein Problem haben...*

Wenn ich kein Problem mit der Öffentlichkeit meiner Daten habe, heißt das nicht, dass damit Andere auch kein Problem haben...*

Wenn ich mit dem Adressbuch einer Person nichts schlimmes anfangen kann, heißt das nicht, dass es egal ist, was damit passiert...

Dies gilt besonders für die Zukunft, evtl. Chefs, Firmen oder andere Kulturen (wie z.B. die USA).*

(Siehe auch unten bei „weitere hilfreiche Fragen“.)

8. Naivität macht Kriminalität erst lohnend

Jede Person die jede e-mail und deren evtl. Anhänge gleich öffnet oder beliebige Apps installiert oder seinem „Virenschutzprogramm“ vertraut, ist eine Gefahr für alle. Wer hingegen im Internet mit einem abgesicherten Browser (NoScript, …) nur vorsichtig auf seriösen Seiten unterwegs ist, bei mails erst ein-zwei Tage wartet und diese vor dem Öffnen erst überprüft, Apps und Webseiten (facebook) keine zu weiten Zugriffe (Adressbuch!) gewährt und lieber mal verzichtet und schweigt, dabei sein System abgesichert/aktuell hält und auf gepflegte und geprüfte OpenSource-Software setzt, verleidet den Kriminellen die Arbeit.

Weiter ...

Auch weitere Problemfelder können in diesem Zusammenhang behandelt werden...

> ***Zum Beispiel:*** *Das Verschicken eines beliebigen Nacktbildes - auch von sich selbst - (oder gar Pornofilms) per WhatsApp, e-mail oder ... an eine minderjährige Person (z.B. den Freund) ist als „Verbreitung von Pornographie“ strafbar!*

Fazit

=> Digitale Kommunikation ist keine „reale“ Kommunikation. Sie verlangt einen bewussteren und umsichtigeren Umgang und sorgfältige Datensparsamkeit. Merkwürdigkeiten sind unbedingt in der realen Welt direkt von Mensch zu Mensch klären. Dabei ist dem bekannten Menschen in der realen Begegnung grundsätzlich mehr zu glauben, als „der Technik“ (= „dumme“ Software von „fremden Menschen“). Nicht: „Warum hast Du nicht geschrieben?“ Sondern: „Ich habe noch nichts bekommen.“

Weitere hilfreiche Fragen:

- Wie lange sind digitale Daten (z.B. Fotos) „haltbar“ bzw. „nutzbar“?

- Wie gut ist die Qualität unserer digitalen Daten?

- Was kann mit dem Material auf unserem Smartphone und unseren „Festplatten“ theoretisch alles angestellt werden? Wie kann dies vermieden werden? Was ist dann die Gefahr? Welches Risiko bleibt?

- Was bedeutet „Vertraulichkeit“?

- Gibt es Dinge, Fotos, Ansichten von uns oder Vorkommnisse, die uns peinlich oder unangenehm sind oder waren? Möchten wir diese öffentlich breitgetreten wissen? Würde dies in einer Freundschaft großzügig weiter erzählt werden? Oder Anderen gegenüber damit sorglos umgegangen werden? Oder eine Bekanntmachung sogar unterstützt werden? Würde es uns Freude bereiten, wenn es jemand anders* Vielen bekannt macht?*

Ergänzung

Stichwörter mit evtl. hilfreichen Aspekten finden sich unter:
http://www.digidaktik.de/research/IT-Sicherheit/Hilfreich-fuer-smarte-Sicherheit.pdf

Weitere Grundlagen

Medienpädagogische Grundlagen wie Betrachtungen über „Medien“ „Medienkompetenz“, „Mediendidaktik“ uvm. finden sich unter: http://www.digidaktik.de/inhalte/da-ph.html .

Personalisierte Pädagogik:
http://www.digidaktik.de/research/Personalisierte_Paedagogik_fuer_Mensch_und_Gesellschaft.pdf

Weitere Unterrichtsideen / Unterrichtsentwürfe:
http://www.digidaktik.de/research/Medienkompetenz-im-Schulunterricht.shtml

Handout zur IT-Sicherheit:
http://www.digidaktik.de/research/IT-Sicherheit/IT-Sicherheits-Checkliste.pdf

Kurzmeldungen:
https://twitter.com/digidaktik

Kontakt für Vorträge / Seminare (und Antworten auf die angesprochenen und weitere Fragen):
http://www.digidaktik.de/referent-medienkompetenz-kontakt.shtml