



Veronika Strauß

Sicher im Netz?!

(Steirische) Jugendliche und ihr Umgang mit sensiblen Daten im Rahmen digitaler Kommunikation

Das Internet stellt für erschreckend viele Erwachsene - sowohl Eltern als auch Lehrpersonen - noch immer ein rotes Tuch, ein Mysterium dar, den erklärten Feind, vor dem Kinder und Jugendliche bewahrt werden müssen. Und das vor allem durch Verbote. Der verantwortungsvolle Umgang damit ist aber erlernbar und notwendig sowohl im privaten als auch im beruflichen Leben. „Das Internet“ ist kein Gegenstand den man wegschließen kann, spätestens seit Web 2.0 und der breiten Einführung mobiler Endgeräte ist es fester Bestandteil des täglichen Tuns. Pathetisch ausgedrückt umgibt es uns, wächst, lebt und lernt durch und mit uns. Im Erkennen und Abwägen von Chancen und Risiken und dem Erlernen technischer Grundfertigkeiten liegt der Schlüssel zum bewussten, kritischen und damit SICHEREN Umgang mit diesem Medium.

Glücklicher Weise ist einem Großteil der (steirischen) Erzieher sehr daran gelegen, ihren Schülern Grundlagenwissen zum sicheren Umgang mit dem Medium Internet zu vermitteln und sich auch selbst zu diesem Thema weiterzubilden. Ein deutliches Zeichen ist die kaum bewältigbare Nachfrage nach den „Sicher im Netz!“ Vorträgen die ich seit Februar 2011 im Rahmen meiner Tätigkeit bei der LOGO Jugendmanagement GmbH anbiete. Über 1000 Schüler haben im ersten Aktionszeitraum (7 Monate) daran teilgenommen und die Termine für das darauf folgende Sommersemester waren bereits vor Weihnachten ausgebucht.

Insbesondere bei Lehrerweiterbildungen wurde augenfällig, dass nicht

nur Bedarf an Sicherheitstipps in Bezug auf das Internet besteht, sondern die meisten (Erwachsene wie Jugendliche) bereits an Wartung und Absicherung des Arbeitsgerätes (PC, Notebook, Smartphone) scheitern.

Jugendliche Lebenswelten

Jeder 5. österreichische User findet die Nutzung von Social Media Diensten über das Handy unverzichtbar.[1] Jugendliche nutzen Online Communities und Location Based Services am stärksten[2].

Für die Schüler meiner Workshops steht wenig überraschend die Plattform facebook an erster Stelle. Laut einer Erhebung[3] der BITKOM von 2011 sind beinahe 100 % der Jugendlichen

zwischen 13 und 18 Jahren mehrmals täglich im Internet. Ähnliche Ergebnisse wurden hinsichtlich der Nutzung von Online Community Angeboten in diesem Altersspektrum publiziert. Gesprächen mit Kollegen aus anderen Bundesländern zu Folge liegt in Bezug auf weitere Social Media Plattformen ein Ost-West-Gefälle vor. In den Bundesländern Vorarlberg, Tirol und Salzburg ist zB das „twittern“ weiter verbreitet als in den östlichen Bundesländern. Die Nutzung von MeinVZ/SchülerVZ/StudiVZ geht zurück und Myspace scheint wieder zum Ursprungszweck (Promotionsfläche für Musiktreibende) zurück gefunden zu haben. Im Media Sharing Bereich regiert allentorts die Video Plattform youtube das Feld. Weiters werden (Online) Games und Web-

sites mit Chatangebot besonders gerne genutzt.

Sich mit den so lebensbestimmenden digitalen Welten der Jugend auseinander zu setzen ist für Eltern, Lehrer und Jugendarbeiter unerlässlich um die nötigen Einblicke zu gewinnen. Pseudo-jugendliche Anbieterung ist aber nicht zielführend, ebenso wenig die Bestrebung Social Media Plattformen als Kontrollinstrument einzusetzen.

Wissen versus Bewusstsein

Augenfällig ist die Tatsache, dass vielen Jugendlichen zwar wesentliche Begrifflichkeiten bekannt sind (Schlagworte wie „Sicheres Passwort“, „phishing“, „Cybermobbing“...) bei näherem Nachfragen aber das vorhandene Wissen nicht im täglichen Tun umgesetzt wird.

Die Gefahr dieser Entwicklung liegt einerseits in der Täuschung, der die Jugendlichen selbst unterliegen („Ich weiß jetzt ‚alles‘, deshalb kann mir nichts mehr passieren!“) und jener der Erwachsenen, die sich beruhigten Gewissens zurücklehnen, da ihre Sprösslinge nun „informiert“ sind. Nicht verinnerlichte „Wissensausschnitte“ und die Tatsache, dass sich im Grunde täglich die Anforderungen ändern und neue Möglichkeiten und Gefahren auftauchen, stellen ein besonderes Risiko dar.

Ein Beispiel für die Diskrepanz zwischen reinem Wissen und dessen bewusster Anwendung ist die schier unglaubliche Ausdauer, mit der Poppers mit Aktualisierungsbegehren von Virenschutzprogrammen „weggeklickt“ werden. („Das ist wichtig, aber ich verstehe es nicht!“ oder „Das ist wichtig, aber ich habe keine Zeit mich damit auseinanderzusetzen.“) Dasselbe Muster ist mir vor wenigen Wochen in Bezug auf eine „Alarmmeldung“ von facebook begegnet, bei der es um die Nichterreichbarkeit der E-Mailadresse des Users ging.

Das Gefühl, dass es hier um etwas Wesentliches geht, ist vorhanden – die notwendige Handlung, das Update des Virenprogrammes, das erneute freischalten der (übrigens bereits gehackten) E-Mailadresse, erfolgt aber nicht bzw. wird automatisiert auf „später“ verschoben.

Noch größer ist das Manko hinsichtlich aktiver Absicherung von mobilen Endgeräten. „Besonders durch die konstante Verbindung zum Internet bieten ungeschützte Handys vielfältige Möglichkeiten für den kriminellen Missbrauch.“[4] Obwohl Unsicherheit – zumindest bei Erwachsenen - spürbar ist, werden bestehende Softwarelösungen zur Verbesserung der Sicherheit im privaten Bereich wenig genutzt.[4]

Meine Erfahrung hat gezeigt, dass das Smartphone nicht als „Computer“ wahrgenommen wird. Dass im Grunde dieselben Sicherheitsvorkehrungen wie für PC und Notebook möglich und notwendig sind, ist nicht allgemein bekannt. Dies gilt nicht nur für die am Smartphone laufenden Programme sondern im Besonderen auch für Schnittstellen: WLAN, Bluetooth und Datenverbindungen über diverse Apps werden völlig unhinterfragt verwendet und sind nicht selten permanent aktiv, was sich nebenbei auch noch enorm nachteilig auf die ohnehin meist schlechte Akkuleistung der Geräte auswirkt. Der bereits zitierte „Mobile Web Watch“ Bericht deckt sich auch hinsichtlich des Sicherheitsempfindens der Jugendlichen mit den Eindrücken aus meinen Vorträgen: Jugendliche haben signifikant weniger Sicherheitsbedenken beim mobilen Internetzugang als Erwachsene.[5]

Eine wesentliche Erkenntnis der ersten Vorträge war, dass das Verhältnis der Jugendlichen zu Dataming und dem daraus resultierenden Werbeangebot in extremem Kontrast zum Empfinden der Erwachsenen steht. Zumeist war es den Jugendlichen egal, wer in den Besitz von Informationen über ihre Interessen und Neigungen kommt. Kann ich Lehrer mit Geschichten über den „gläsernen Menschen“ und „Datenkraken“ - wie erwartet – schockieren, so sind die Jugendlichen der Erhebung von Daten durch z.B. Werbefirmen teils sogar positiv gegenüber eingestellt: „Na, dann bekomme ich wenigstens die Werbung, die mich interessiert!“

Diese Menschen wurden, im Unterschied zu den vorangegangenen Generationen, mit dem stückchenweisen Abgeben von persönlichen Informationen sozialisiert. Jeder Free-Mail-Anbieter fragt Neigungen ab, jede Such-

anfrage über eine Suchmaschine ist wieder ein weiteres marktanalytisches Puzzlestück in einer Datenbank. Und Plattformen wie facebook sind – laut dem Kabarettisten Michael Niavarani – ohnehin nichts anderes als „Stasi auf freiwilliger Basis“. Gäbe es kein Bedürfnis, sich öffentlich oder halböffentlich zu präsentieren, sich ein „Profil“ zusammen zu bauen, wären Social Media Anwendungen, egal welcher Ausrichtungen, nicht so erfolgreich. Es gibt also Bedarf an Raum für Selbstdarstellung im Internet. Ein menschlicher Zug, der bei all diesen Betrachtungen berücksichtigt werden muss.

Stolpersteine

Das Konzept der Vorträge „Sicher im Netz?“ fußt auf Bewusstseinsbildung für Chancen und Risiken und konkreter, praktisch anwendbarer Information. Die folgenden sechs Erkenntnisse bilden den Grundstock für einen bewußten Umgang mit dem Internet:

- Im Internet ist man NICHT anonym!
- Das Internet vergisst nicht![6]
- WENIGER ist MEHR! Was gar nicht erst im Netz landet, kann einem nicht zum Verhängnis werden
- Das Internet ist KEIN rechtsfreier Raum!
- NICHTS ist wirklich GRATIS!
- Erst DENKEN, dann KLICKEN!

Anhand von lebensnahen Beispielen und Geschichten werden die Herangehensweisen den Jugendlichen näher gebracht.

Viele Fehlhandlungen gründen auf Halbwissen oder Fehlinformation. Wie zum Beispiel die sich hartnäckig haltende Annahme, dass von einer Internetseite gelöschte Inhalte unwiederbringlich gelöscht sind. Dass das erstens meist nicht der Fall ist und zweitens diese Inhalte schon hundertfach von anderen Personen heruntergeladen, gescreenshotet und gespeichert worden sein können und man bereits beim Einstellen ins Internet die Kontrolle über diese Daten völlig aus der Hand gegeben hat, daran wird nicht gedacht.

Grundsätzlich ist es angezeigt nicht in außergewöhnlichen Situationen im Internet aktiv zu werden (Liebeskum-

mer, Lotto-6er, Trunkenheit, Übermüdung,...) und IMMER RISIKO und NUTZEN abzuwägen. Um einen Überblick über die eigenen Internetpräsenz zu er- und behalten ist es notwendig, sich regelmäßig zu „suchen“ (Metasuchmaschinen, Personensuchmaschinen).

Kommunikation und Nutzung von Angeboten

Nicht mehr benötigte user accounts (allen voran „alte“ myspace-Profile und E-Mail-Konten) werden meist nicht gelöscht, sondern einfach „vergessen“. Dort platzierte Informationen tauchen erst Monate oder Jahre später wieder peinlich „aus dem Nichts“ auf, wenn nach dem eigenen Namen – bzw. nach den Namen von (Klassen)Kollegen gesucht wird. Je länger ein account inaktiv brach liegt, desto schwieriger wird es, die noch vorhandenen Daten zu „löschen“ bzw. den account still zu legen. Die Zugangsdaten sind inzwischen meist längst vergessen oder die Plattformen nicht (mehr) administriert.

(Gratis)Angebote müssen hinterfragt werden: Wer sind die Ersteller/Nutznieser? Welche „Stolpersteine“ verstecken sich in AGBs und Datenschutzrichtlinien?

Auch bei der Kommunikation via E-Mail passieren weitreichende und wirkstarke Fehler. Das unüberlegte Öffnen von attachments und links und das wahllose und unreflektierte (nicht als blind copy!) Weiterleiten von Nachrichten (auch SMS und private messages) ist der Ausgangspunkt für erfolgreiches phishing, Spamattacken, datamining und die Verbreitung von Schadprogrammen.

Geräteschutz und Zugangsdaten

Wie Eingangs erwähnt, besteht bei der Absicherung und Wartung der Endgeräte enormer Handlungs- und Informationsbedarf. Installieren und regelmäßiges aktualisieren von Schutzprogrammen (sowohl system- als auch browserbezogen), das Verwenden von in den Berechtigungen abgestuften Benutzerkonten, das Kreieren und Einsetzen von UNTERSCHIEDLICHEN, sicheren Passwörtern und die Geheimhaltung eben dieser sind nur einige wenige der notwendigen Maßnahmen.

Sensible Daten und Daten anderer

Ein besonders markanter Punkt der Bewusstseinsbildung ist die Verdeutlichung, dass – im Besonderen auf Plattformen wie facebook – jeder auch Verantwortung für die Daten(sicherheit) der Anderen trägt. Sensible Daten (dazu gehört zB auch die Schule, die ein Jugendlicher besucht!) müssen geheim gehalten werden und dürfen auch an „Freunde“ nicht ohne Rücksprache mit dem Dateninhaber weiter gegeben werden. Gerade bei Fotos wird dies oft nicht eingehalten.

Offenes WLAN / Öffentliche Rechner / Verbindungen

Vom Verwenden von nicht passwortgeschützten Internetzugängen ist abzuraten und an öffentlich zugänglichen Rechnern sollten keine Zugangsdaten eingegeben werden.

Facebook-spezifische Handlungsrichtlinien werden in den Workshops sehr detailliert behandelt, würden aber den Rahmen des Artikels um ein vielfaches sprengen.

Was die „Stoppersteine“ bzw. deren Umgehung im Detail ausmacht, kann in INFOmaterialien der LOGO JUGEND.INFO nachgelesen bzw. bei einem persönlichen Termin erörtert werden.

Was können wir tun?!

Ja, das Internet bietet nicht nur Chancen, sondern birgt auch Risiken, sogar ernstzunehmende Gefahren. Ja, es ist wichtig gerade junge Menschen darüber aufzuklären, WELCHE Risiken das sind, und wie sie sich und ihre Mitmenschen davor schützen können. Ja, das Gros der Jugend, aber auch viele Erwachsene sind unbedarft, um nicht zu sagen leichtfertig in ihrem Umgang mit dem Internet und ihren persönlichen Daten.

Was also können wir tun? Wie bereits am Beginn des Artikels angemerkt, hilft die relevanteste und qualitativ hochwertigste Information NICHTS, wenn sie die Person, die sie aufnehmen soll, nur streift. Auch blankes WISSEN ist zu wenig, wenn der Konnex zum „realen Leben“ fehlt. Nicht nur den Jungen – uns allen muss

BEWUSST werden, dass wir täglich selbst das Monster füttern, vor dem wir uns so fürchten. Erst mit dem Bewusstsein für das eigene Handeln, ist es möglich dieses Monster zu zähmen und verantwortungsvoll und nachhaltig risikoarm damit umzugehen. Das schließt die, zumindest gedankliche, Beteiligung an gesamtgesellschaftlich relevanten Diskussionen wie Datenschutzverordnungen und dergleichen ein. Lebenswelten sind Medienwelten, sagte Dieter Baacke (Medienwissenschaftler). Also müssen wir uns auch dafür einsetzen, dass unsere Medienwelten lebensWERT sind!

Ohne das Vorleben des obgenannten, egal ob in der Schule, am Arbeitsplatz, zu Hause oder im Freundeskreis wird es niemandem gelingen, die nötige Ernsthaftigkeit zu transportieren um eben diesen bewussten Umgang glaubwürdig vermitteln zu können.

Wenn dies durch passende Bildungsangebote unterstützt werden würde, wäre bereits ein großer Schritt in Richtung Datensicherheit/Datenschutz getan. Und ein weiterer hin zu mehr Selbstverantwortung und letztlich demokratischem Handeln.

Die LOGO JUGEND.INFO setzt 2 kostenlose Angebote:

- Vorträge/Workshops für Jugendliche und Multiplikatoren
- facebook-check (das gemeinsame Durchgehen des persönlichen Accounts hinsichtlich Sicherheitseinstellungen)

Zum Abschluss – Fangen wir an!

Nicht jeder interessiert sich für die Entwicklungen im und um das Internet im Detail und das kann auch von niemandem verlangt werden. Eine verlässliche Strategie, die sicherstellt, dass „lebensnotwendige“ Basisinformationen von den Usern (und das sind wir letztlich ALLE) nicht nur gehört, sondern auch verstanden und angewendet werden und, dass diese Informationen immer wieder auf Richtigkeit überprüft und ggf. aktualisiert werden, wäre notwendig! Den Eltern kann man es nicht zumuten (oder zutrauen) – das Bildungssystem müsste wieder einmal herhalten. Oder es wird auf externe Schulungen gesetzt. Dabei stehen si-



**Mag.
Veronika Strauß**
Informationsberaterin
bei LOGO Jugendma-
nagement GmbH

Dr. Michael Wesch mit dem Menschen im digitalen Zeitalter (Digital Anthropology, <http://mediatedcultures.net>).

Unter dem nachfolgenden Link finden Sie eine – wie ich finde – formvollendete Einführung: „THE MACHINE

2008 Abschluss des Studiums der Volkskunde und Kulturanthropologie an der Karl-Franzens Universität Graz mit Auszeichnung. Diplomarbeit zur Arbeitervolkskunde (Arbeitskräfteüberlassung), ausgezeichnet mit dem Förderpreis für wissenschaftliche Arbeiten der Arbeiterkammer Steiermark. Zahlreiche Publikationen für LOGO Jugendmanagement GmbH. www.xing.com/profile/Veronika_Strauss4 veronika.strausz@logo.at

cherlich die fachlichen Kompetenzen, aber – und das ist der Unterschied zwischen dem reinen „einfüllen“ von Information in jugendliche Köpfe und der tatsächlichen WissensVERMITTLUNG – vor allem auch die pädagogischen Fähigkeiten, die Authentizität, die Fähigkeit, mit den Jugendlichen in IHRER Lebenswelt, glaubwürdig und auf Augenhöhe kommunizieren zu können, im Vordergrund!

Eine Aufgabe, die nicht leicht zu bewerkstelligen, jedoch von nachhaltigem Wert und Wichtigkeit für Arbeits- und Privatleben aller ist, weswegen sie hier auch Erwähnung findet.

In großartiger Weise beschäftigt sich der US-amerikanische Wissenschaftler

IS US/ING US“: <http://ksuanth.weebly.com/wesch.html>

Autor:

Mag. Veronika Agnes Ursula Strauß ist derzeit als Informationsberaterin bei der LOGO Jugendmanagement GmbH beschäftigt. Zu den Kerntätigkeitsbereichen zählen unter anderem Schulungen für Jugendliche und Multiplikator (Jugendarbeiter, LehrerInnen) zum sicheren Umgang mit dem Internet.

Seit 2000 laufend Fortbildungen v.a. zu den Themengebieten Social Media, Qualitätsmanagement, Statistik, Publikationsrecht, Meinungsforschung und Öffentlichkeitsarbeit.

Referenzen:

- 1 Mobile Web Watch 2011 Deutschland, Österreich, Schweiz. Die Chancen der mobilen Evolution., S.19. (http://www.accenture.com/SiteCollectionDocuments/Local_Germany/PDF/Accenture-Studie-Mobile-Web-Watch-2011.pdf, 14.12.2011)
- 2 Mobile Web Watch 2011, S.5.
- 3 Jugend 2.0. 10- bis 18-Jährige in der digitalen Welt. Prof. Dr. August-Wilhelm Scheer. BITKOM-Präsident. Pressekonferenz. 26. Januar 2011, Berlin; S.8, 29.07.2011.
- 4 Vgl. Mobile Web Watch, S.29.
- 5 Mobile Web Watch, S.29.
- 6 Siehe dazu auch www.wayback-machine.org

Call for Papers

Themenschwerpunkt: Logistikplanung

in WINGbusiness 03/2012

Beschreibung

Für die Ausgabe 03/2012 laden wir Autoren ein, wissenschaftliche Artikel (WINGPaper) zum Thema „Logistikplanung“ einzureichen.

Steigende Leistungskriterien, volatile Märkte, hohe Produktvielfalt und komplexe Prozesse stellen aktuelle Herausforderungen für die Logistik dar. Gleichzeitig müssen Kapazitäten bedarfsgerecht bereitgestellt werden, Leer- und Opportunitätskosten vermieden werden.

Von Interesse sind Arbeiten zum Thema flexibler Planung von logistischen Systemen und Prozessen, auf allen Ebenen und Bereichen von der Infrastruktur über die zwischenbetriebliche Koordination bis hin zu Materialfluss- und Lagersistemen.

Hinweise für Autoren:

Vorlagen zur Erstellung eines WINGpapers und konkrete Layout-Richtlinien sind als Download unter: <http://www.wing-online.at/services/wingbusiness/medienfolder.html>

oder per E-Mail verfügbar. Autoren können ihre Beiträge zum Themenschwerpunkt als PDF an office@wing-online.at übermitteln.

Die Ergebnisse des Reviews werden dem Autor innerhalb von 4-8 Wochen nach Einsendung des Artikels zugestellt.

Annahmeschluss: 09.07.2012