



„Datenschutz im Alltag / Digitale Selbstverteidigung heute“

Andrea 'Princess' Wardzichowski
Chaos Computer Club Stuttgart e.V.

<http://www.cccs.de/>
princess@bofh.de

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

1

Mein Vortrag beginnt mit meinem Nickname. Nur durch dessen (Mit-)Verwendung kann ich andeuten, daß ich privat unterwegs bin.

...hat mich jemand vor dem Vortrag gegooglet? :-)

Über den CCCS / über mich

CCCS:

seit Sommer 2001: Stammtisch-Treffen
seit Oktober 2003/4: monatliche Vortragsreihe
(Seit 2009 in der Stadtbibliothek)
Spaß am Gerät, aber auch: Gefahren durch
bedenkenlosen Einsatz von Technik

Princess:

seit November 1990 im Netz aktiv
(IRC, Mail, NEWS, Relay Parties, CCC)
heute: CCCS (Presse), Haecksen,
Vorträge bei Informatica feminale 2013, DiB Tagung 2013,
querulantin.de

Aufgrund langjähriger Erfahrung im Internet und beim CCCS bin ich heute hier, um meine **Erfahrungen** mit Ihnen zu teilen.

Der CCCS hat bereits mehrere Jahre lang eine Kooperation mit der Stadtbibliothek, weswegen der heutige Termin in Vaihingen auch zustandekam.

Über mich:

Andrea 'Princess' Wardzichowski bewegt sich seit November 1990 im Internet und hat die Entwicklung des Internets von einem rein akademischen Netzwerk der Vor-WWW-Zeit zu einem Massenmedium verfolgt. Seit 2001 engagiert sie sich beim Chaos Computer Club Stuttgart e.V. und tritt dort auch für „Spaß am Gerät“ ein, aber doch auch für Umsicht im Umgang mit Daten und Technologie ein und versieht die Arbeit der Pressesprecherin. Der Datenschutz inner- und außerhalb des Netzes ist hierbei das Hauptthema.

Ein weiteres Anliegen ist ihr auch die Frauen- und Mädchenförderung im technischen und naturwissenschaftlichen Bereich.

Hauptberuflich ist sie in der Technikabteilung eines nichtkommerziellen Internetproviders beschäftigt.

Agenda

- Datenschutzgesetz
- Datensammlung per Gesetz
- Datenabgaben, denen man kaum entkommt
- Freiwillige Datensammlungen
- Gefahren von Datensammlungen
- Was tun?

Wir wollen heute erörtern, wo in einem normalen Leben in Deutschland personenbezogene Daten in Deutschland gespeichert werden.

Sodann wird diskutiert, welche Daten im Netz gespeichert sind und wie man dies in Zukunft minimieren, wenn auch nicht zu 100% verhindern kann.

Es werden praktische Hinweise und Ansatzpunkte gegeben.

Datenschutzgesetz

- Bundesdatenschutzgesetz
- Landesdatenschutzgesetze
- Angepasste Datenschutzgesetze
- Zweckbindung bei der Datenerhebung
- Datensparsamkeit
- Datenschutzbeauftragter (Bundes-, Landes-, Firmen, KK, öffentliche Stellen, Schulen, Hochschulen...)
=> Volkszählungsurteil, Informationsfreiheitsgesetz, Transparenz bei der Verarbeitung von **personenbezogenen Daten**
=> EU-Datenschutzverordnung Mai 2018

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

4

Hier in der Bundesrepublik Deutschland gilt so gut wie überall eines der **Datenschutzgesetze**, die **personenbezogene Daten**, deren Speicherung und Verarbeitung, schützen.

Grundsätze sind hierbei immer eine **Zweckbindung** bei der Erhebung von Daten (sie dürfen nicht anlaßlos erhoben werden), sowie die **Datensparsamkeit** (es dürfen nur die Daten erhoben werden, die für einen Zweck auch notwendig sind).

Jede Stelle, die personenbezogene Daten speichert, muß einmal im Jahr **kostenlos Auskunft** darüber geben, welche Daten sie gespeichert hat (auch die Schufa! Die verlangen ganz frech trotzdem Gebühren).

Allerdings nimmt nicht jede Stelle und nicht jede Firma es so genau mit dem Datenschutz: gelegentlich muß man einmal **nachfragen**, ob alles mit rechten Dingen zugeht, notfalls auch öfter als einmal. **Verstöße** können beim Landes- und Bundesdatenschutzbeauftragten gemeldet werden! (Habe dies auch schon gemacht!)

Firmen und öffentliche Stellen müssen zudem einen eigenen Datenschutzbeauftragten bestellen, der für Anfragen dieser Art zur Verfügung stehen muss!

Was aber ist mit Firmen, die ihren Hauptsitz und ihre **Server und Speicher nicht in Deutschland** stehen haben? Hier ist Vorsicht geboten! Wir kommen noch darauf zurück.

Datensammlung per Gesetz

- **Einwohnermeldeamt**
- **Pass, Personalausweis** (RFID, Biometrie)
(beim neuen Perso keinesfalls Fingerabdrücke abgeben, das ist optional!)
- **Rundfunkbeitrag** (früher: GEZ), heute pro Haushalt, nicht nach Geräten erhoben, Meldeämter geben Daten weiter (Passus im Meldegesetz)
- **Krankenkasse** (Pflicht, auch wenn sich nicht jeder den Wiedereintritt leisten kann!)

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

5

Wenn man in Deutschland lebt, kommt man nicht darum herum, einige seiner **Daten von Gesetzes wegen abzugeben**. Ich habe zu diesem Zweck auch einmal das Meldegesetz gelesen. Das Lesen von Gesetzestexten ist für Nichtjuristen zugegebenermaßen schmerzhaft, aber für eine CCCS Referentin gelegentlich notwendig ;-)

Zwischenfrage: muß man einen Ausweis mit sich tragen?

Nein! Man muß nur Perso oder Paß besitzen, der darf aber zuhause liegen. Aus praktischen Erwägungen ist es aber besser, ihn bei sich zu haben.

Der **Rundfunkbeitrag** wird nunmehr pro Haushalt erhoben, es gibt meines Wissens fast keine Möglichkeit, diesen nicht zu entrichten. Es gibt einen Vorteil des Systems: die „Klinkenputzer“, die Nichtzahler zuhause aufgespürt haben, wurden von den Sendeanstalten entlassen. Hier gab es immer wieder abendfüllende Zwischenfälle am Rande der Legalität.

Inzwischen herrscht auch **Krankenkassenpflicht**. Die Krankenkasse hält besonders **intime und heikle Daten** vor. Daher muß man auch die Entwicklung der neuen **Krankenkassenkarte** sehr genau beobachten. Geht hier die Sicherheit flöten, ist der Zugriff und vielleicht auch die **Änderung von Gesundheitsdaten möglich!** Das Bild alleine auf der neuen eGK hilft übrigens gegen fast nichts, das war nur eine teure Aktion und wird den Mißbrauch nicht eindämmen.

Datenangaben, denen man kaum entkommt

- **Bank** (sowie Schufa und ähnliche)
- **Telekommunikationsanbieter** (Festnetz, mobil)
- **Videoüberwachung** (ÖPNV, Verkehrskameras)

Nicht zwingend notwendig, aber bequem:

- Versandhandel
- Rabattsysteme (Bahncardpunkte, Payback, ..)

Ob Erwerbseinkommen oder Sozialleistungen, Rente, Unterhalt: ohne ein **Konto bei einer Bank** kommt man heute idR. nicht aus. Die Bank weiß viel: sie weiß wo das Geld herkommt, und sie weiß, wo es hingeht.

Ich rate dazu, **Kartenzahlungen** (EC-, Kredit-, Geld-) zu **vermeiden**. Jede Kartenzahlung verursacht eine Datenspur. Die Bank sieht wo und wann Einkäufe getätigt wurden.

Weiterhin ist es heute ziemlich unmöglich, keinerlei **Telefon** zu haben. Der Telekommunikationsanbieter kennt, zumindest für einen gewissen Zeitraum, alle **Kommunikationspartner**. Im Falle von Mobilfunk auch den Sendemast, an dem ein Mobiltelefon eingebucht ist. Zumindest **grobe Lokalisierung** wäre so möglich.

Nicht entkommen kann man der allgegenwärtigen **Videoüberwachung**. Man kann aber bei allen speichernden Stellen **Auskunft verlangen**, wie lange die Aufzeichnungen gespeichert werden. Wenige Tage sind zur Aufklärung von Sachbeschädigung und Belästigung in öffentlichen Fahrzeugen vertretbar. Ist hingegen nichts vorgefallen, sollten die Aufnahmen auch zeitnah gelöscht werden. Trauen Sie sich, fragen Sie nach!

Das Leben leichter macht in vielen Fällen der boomende **Versandhandel**. Hier lassen sich aber aus den bestellten Artikeln auch Verhaltensprofile erstellen. Bei **Amazon** kann man aber z.B. einstellen, daß möglichst wenig gespeichert wird.

Freiwillige Datensammlungen / Internet

- Webseite
- Blog
- Teilnahme an Foren (früher News/Usenet), Leserbriefe
- Social Media (facebook, twitter, Xing, whatsapp) hier auch: Verbreitung von Fotos!
- Wunschliste bei Amazon....
- Webseiten von (Sport-)Vereinen
- Nicht unterschätzen: social hacking

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

7

Völlig freiwillig ist hingegen die **aktive Teilnahme** am Internet. Wer nur Webseiten sichtet und private E-Mails schreibt, hinterläßt zwar auch an vielen Stellen **Datenspuren**, die wenigsten davon sind aber öffentlich.

Wer **aktiv Inhalte ins Netz stellt**, diskutiert oder Fotos veröffentlicht, sollte sich überlegen, ob er/sie dies mit seinem **richtigen Namen** tun will und wieviel davon **die Welt** wirklich wissen muss.

Denkfalle ist oft, daß man das nur „für Freunde und Familie“ schreibt/veröffentlicht. In Wahrheit sind viele Dinge, auch aus sozialen Netzwerken, für die Welt lesbar.

Denkanstoß: Nehmen Sie ein Stück alte Tapete und kreieren Sie darauf Ihre „Homepage“ und lassen Sie dies auch Ihre Kinder tun. Danach meditieren Sie gemeinsam darüber, ob Sie das Werk im Hausflur eines Mietshauses, auf der Straße vor dem Haus oder an der Bushaltestelle für alle sichtbar aufhängen würden, mit der Folge, daß JEDER, Freund und Feind, die Infos lesen kann. Auch: **welche Schlüsse** auf den Geschmack und die Vorlieben könnte jemand aus der Amazon Wunschliste ziehen?

Unterschätzt wird die Gefahr bei **Webseiten von Sportvereinen**. Während Schulen inzwischen gelernt haben, keine erkennbaren Fotos und Namen zu veröffentlichen, sind Kinder über Ihre Sportvereine oft **leicht find- und stalkbar**. Denn: Die Vereine freuen sich ja, wenn jemand an Wettbewerben teilnimmt etc.pp. Klären Sie auf!

Social hacking: aushorchen des Gesprächspartners durch lockere Plauderei. Buchtip: die Trilogie von Stieg Larsson.

Freiwillige Datensammlungen / mobil

- Nicht zu vermeiden: an welcher Funkzelle ist ein Mobiltelefon eingebucht?
- GPS: muss nicht ansein
- Internet dito
- Lokalisation auch anhand von WLANs möglich, die das Smartphone aktuell angeboten bekommt
- GPS-Daten als EXIF-Daten in Bildern!

Wer sich Zugang zu der Technik eines Mobilfunkproviders verschaffen kann, hat Zugriff darauf, welches Gerät sich wo befindet. Das geht idR. Aber niemanden etwas an.

Überlegen Sie, ob Sie Internet und GPS permanent brauchen?

Navigation mit OpenStreetmap (App „osmand“) ist auch ohne Internet möglich (offline Karten herunterladen).

Überlegen Sie auch: wieviele Apps, die Internet und GPS brauchen, **brauchen SIE wirklich und dauerhaft?**

Auf eine weitere „Falle“ wurde ich aufmerksam, als ich einen Vortrag für „Frauen helfen Frauen e.V.“ vorbereitete (diese betreiben das Frauenhaus):

Wenn man Bilder mit dem Smartphone macht und das GPS ist an, dann werden die GPS Koordinaten in den Metadaten der Bilder abgelegt. Lädt man diese Bilder irgendwohin hoch, könnten die GPS Daten Auskunft über den Aufenthaltsort geben: wenn man gerade seinem Partner „entkommen“ ist, keine gute Idee (und auch sonst nicht, wen geht es etwas an, wo ich ein Foto mache).

Gefahren von Datensammlungen

.....nix zu verbergen?

Bin ICH denn interessant für
irgendwen?

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

9

Wenn ich von Vereinen oder Parteien eingeladen werde, gibt es im Auditorium häufig einige Menschen, die diese These vertreten. Ich zeige dann auf, daß es unendlich viele Dinge des Privatlebens gibt, die **weder verboten** (strafbewehrt oder ordnungswidrig) **noch anrücklich** sind, die man aber dennoch nicht sofort jedem erzählen mag.

Fragen zur Selbstreflektion:

- warum habe ich Gardinen an den Fenstern?
- warum schließe ich für bestimmte Tätigkeiten/Verrichtungen Türen?
- warum erzähle ich nicht jedem, wieviel ich verdiene?
- warum erzähle ich nicht jedem, welche Krankheiten ich habe? (Erb-, chronische, Geschlechtskrankheiten....)
- warum beichte ich nicht dem Finanzamt meine Steuertricks?

Auch für den Arbeitgeber wird eine zu große Aktivität in sozialen Medien genau DANN interessant, wenn er einen loswerden will (z.B. durch Posten in der Arbeitszeit).

Wann bin ich interessant?

- Strafverfolgung (klar)
- Arbeitgeber?
- Partner/Expartner?
- Stalker
- Klatsch/Tratsch/Gerüchte/Rufschädigung?
Nicht nur Prominente sind betroffen!
Jeder hat ein soziales Umfeld (auch Nachbarn, Kollegen, Freunde, Vereinspartner, Familie...)
- Auch: Punkte in Flensburg anhand von facebook Bildern?

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

10

Die **Strafverfolgungsbehörden** können natürlich auf alle existenten Datensammlungen (in .de) zugreifen. Dies ist zwar legitim und verständlich, aber auch hier gilt: Daten über mich, die es nicht gibt, kann auch niemand gegen mich verwenden.

Der **Arbeitgeber** könnte, wie eben schon angedacht, prüfen, ob man während der Arbeitszeit andere Dinge tut (facebook, twitter).

Nicht schön, aber im richtigen Leben kommt es auch zu **Trennungen zwischen Partnern**. Man möchte idR. nicht, daß der/die Ex weiter weiß, was man so tut, egal wie friedlich die Trennung vor sich ging.

„Gerüchte zu widerlegen ist so, wie zu versuchen, Zahnpasta in die Tube zurückzudrücken. Es gibt nur eine Riesensauerei“.

In meinem Umfeld: Firma gleichen Namens begeht immer wieder **Geschwindigkeitsübertretungen** und ein bekannter wird beschuldigt. Er sagt, er war in seinem LEBEN noch nicht in Bochum. „Doch, sie WAREN das, wir haben Sie anhand Ihres facebook Profils identifiziert“.

Es ist nicht verboten, auf öffentliche Bildersammlungen zurückzugreifen. Besser, man hat kaum Bilder im Netz.

Verbrechensbekämpfung als Zweck?

- Umkehr der **Unschuldsvermutung** (Vorratsdatenspeicherung (derzeit wird Nichterfüllung nicht angezeigt,) großer Lauschangriff)
- Daten, die einmal erhoben sind, werden auch genutzt
- Nicht alles sind „**Maßnahmen gegen den Terror**“! Immer noch aktuell: Einführung von RFID Chips im Pass und biometrischen Personalausweisen, Einschränkung von Freiheitsrechten ohne Nachweis, daß es auch etwas bringt
- **Rasterfahung?** War die jemals erfolgreich? (RAF bis heute!)
=> **kaum Erfolgskontrolle** bei Datensammlungen bzgl. Strafverfolgung
=> Daten, die es nicht gibt, können nicht mißbraucht werden oder verlorengehen

Die **Abkehr von der Unschuldsvermutung** geschieht schleichend. Jede Maßnahme und jedes Gesetz einzeln, das nach dem 11. September 2001 erdacht wurde, stellt vielleicht keine Gefahr für die Bevölkerung dar. Aber die Gesetze werden immer mehr und man wird immer mehr beobachtet, überwacht und ausgespäht. **Spätestens seit Snowden** wissen wir, was auch noch die Geheimdienste, meist völlig ohne parlamentarische Kontrolle, sich erdreisten.

Die **Vorratsdatenspeicherung** ist derzeit außer Kraft (war EU Richtlinie) und die Strafverfolgungsbehörden weinen laut. Aber: auch vor Inkrafttreten der VDS wurde mit Hilfe von **anderen Ermittlungsverfahren** die „Sauerlandzelle“ enttarnt. Es ist nicht so, als seien wir ohne die VDS komplett hilflos.

Leider wird in Strafverfahren nicht so richtig gemessen und erfasst, welche Maßnahme wieviel bringt. Alle Bürger **präventiv in Sippenhaft** zu nehmen, denn sie könnten ja irgendwann straffällig werden, ist jedenfalls **in einer Demokratie keine Lösung!**

Konsequenzen in der Zukunft?

- Prognosen sind immer schwierig, insofern sie die Zukunft betreffen!
- Nicht alles, was ein Mensch heute vertritt, ist ihm auch morgen noch nicht peinlich
=> Miley Cyrus, Politikerin der AFD
- Meinungen können sich ändern, z.B. Real Name Pflicht im Internet (habe ich früher vertreten, tue ich heute nicht mehr)
- Jugendliche können Konsequenzen NOCH schlechter abschätzen als Erwachsene
- Eltern sind in der Pflicht: sollen spätere Arbeitgeber, aber auch Partner im Internet alle Kinderbilder einsehen können?
- Ganz banal: angekündigte An-/Abwesenheit kann durch Einbrecher ausgenutzt werden.

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

12

Auch aus meiner Biografie: **man entwickelt sich weiter** und darf seine Meinungen auch ändern! Im Gegenteil, ein Beharren an inzwischen als falsch erkannten Thesen ist ziemlich albern (aber passiert, s. Sommerzeit.....).

Selbst Kinderstars wie **Miley Cyrus**, die ihr ganzes Leben vermutlich von Beratern umgeben waren und sind, begehen Fehler: so sagte Miley Cyrus jüngst im Frühjahr 2017, daß das Video mit ihr nackt auf einer Abrißbirne ein Fehler gewesen sei, weil jeder sie nun genau so in Erinnerung habe.

Auch und ganz **ohne moralische Bewertung**: eine Politikerin der AFD war vor ihrem Mandat bei einer **Escort-Plattform** angemeldet und unterwegs. Das Profil existiert nicht mehr, findet sich aber noch in den Archiven der Suchmaschinen. Man entkommt seiner Vergangenheit also nicht, wenn sie einmal im Internet war.

Eltern sollten wirklich reflektieren, welchen Schaden eine lückenlose „**Bilderbiographie**“ im Internet später mit ihren Kindern für Schaden anrichten kann.

Sicher kann man heute auch herausfinden, daß ich mich vermutlich zwischen 16 und 20 Uhr nicht im Hause befinden werde, aber ich mache es Einbrechern nicht noch leichter durch mein Blog (facebook habe ich nicht) indem ich ankündige, wann ich so sein werde.

Vor- und Nachteile der mobilen Kommunikation

- Zunächst: das Internet ist ein wunderbarer Raum zum **Kommunizieren** und zur **Wissensgewinnung!**
- „früher“: alle Freunde durchtelefonieren.
Heute: alle per facebook oder whatsapp einladen
- Auch: **Sportvereine** haben keine „Telefonkette“ mehr. Aber hat auch **jedes Kind unbeschränkt Internetzugang?**
- Werden Menschen ohne Smartphone **abgehängt?**
- Bekommen Menschen ohne Internetzugang **weniger Rabatte?**
- Datenspuren (Äußerungen, Fotos)
- Daten liegen oft **im Ausland unter unklarer Rechtslage!**

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

13

Noch nie war es so leicht, **an Wissen zu gelangen**, wie heute. Früher endete mein Wissenshunger an dem Füllstand der Hamburger Öffentlichen Bücherhalle. Mehr als dort war für mich nicht zugänglich. Heute kann man auf unzählige Wissensdatenbanken zugreifen. Kernkompetenz ist zweifellos **„gut suchen“ können und die Bewertung von Quellen.**

Wenn man sich an **gewisse Regeln** hält, kann man viel Spaß haben und auch viele tolle Menschen kennenlernen. Die „Regeln“ sollten wie Verkehrsregeln begriffen werden. Diese hat man verinnerlicht und man begreift sie auch nicht als Last, sondern einfach als sinnvoll.

Wichtig: das Leben muß auch ohne Internet lebbar sein, ohne Nachteile! Nicht jeder will und kann am Internet teilnehmen. Manche Menschen haben nicht das Geld, einen Rechner und Internetzugang zu unterhalten. **Dafür gibt es hier in der Bibliothek Leihrechner!**

Suchtgefahren

- „**Muß man immer mal hingucken**“
(Definition „Smartphone“ einer Dreijährigen)
- Persönliche Erfahrungen im Bereich Online-Dating
- ...plötzlich bekommt man *Komplimente* für Fotos.
- Kein Wunder, daß Jugendliche „likes“ wollen
- **Eltern**: ausprobieren! Mailadresse unter anderem Namen anlegen und sich in einer Plattform anmelden. Sodann jeden Tag (!) eine halbe Stunde dort oder im Chat verbringen. 14 Tage lang.
- „Das sind doch keine Fremden!“

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

14

Ich **chatte seit November 1990**. Was früher die Beschäftigung im Rechnerraum abends vor dem Ausgehen war, begleitet mich heute oft. Aber: wenn ich unterwegs bin oder gar im Urlaub **muß das Internet auch mal ohne mich auskommen!** Ich bin dann auch per Mobiltelefon nur für Notfälle erreichbar. Freunde und Familie wissen das!

Durch Partnersuche im Internet habe ich aber auch selber gemerkt, wo das **Suchtpotential** liegt! Jede/r ist da anders, **mancher anfälliger** als der/die andere. Insbesondere aber Kinder und Jugendliche haben für viele Dinge noch nicht **das rechte Maß**. Dies muß man ihnen vorgeben und auch vorleben.

„**Das sind doch keine Fremden**“: Kinder und Jugendlichen kann man sehr gut plausibel machen, nicht mit fremden Menschen mitzugehen oder gar zu ihnen ins Auto zu steigen. Aber: ihre **Chatfreunde SIND keine Fremden!** Probieren Sie es aus, halten Sie sich 2-3 Wochen jeden Abend im selben Chat auf. Sie verraten weder ihren richtigen Namen noch ihren Wohnort, aber es baut sich dennoch aus dem Geplänkel über „Alltagsscheiß“ **irgendwann Nähe** auf. Sie wissen, daß Sie Ihr Gegenüber NICHT kennen. **Kinder können das nicht einschätzen!**

Was tun im richtigen Leben?

- **Datensparsamkeit leben:**
Eintrag im Telefonbuch notwendig?
Adresssperre beim Bürgerbüro möglich (einfache Form)
- **Formulare:**
Trauen Sie sich: füllen Sie nicht alles aus!
Telefonnummer ist nicht immer nötig.
Besondere Vorsicht gilt beim Geburtsdatum.
Neulich im Elektromarkt: Kunden werden bei einem
normalem Einkauf nach Name und Wohnadresse gefragt.
Wozu????
- **Unbedenklich:** Postleitzahl im Laden nennen, wenn man
nicht per Karte bezahlt (rein anonyme statistische Daten)

Ich habe hier in Stuttgart noch nie im **Telefonbuch** gestanden, bekomme aber in Abwesenheit reichlich komische Anrufe. Der Anrufer muss zwar seit einigen Jahren gesetzlich vorgeschrieben seine Nummer übermitteln, dies nützt aber nichts, wenn dann die **Rückwärtssuche** fehlschlägt und man die Nummer nur durch Suchen auf „**Beschwerdeplattformen**“ findet.

Vorteil von telefonieren über VoIP: man kann man Router leicht Nummern sperren, davor war das nur durch eine kostenpflichtige Schaltung beim Telefonprovider möglich.

Hinterfragen Sie Formulare und Menschen, die Ihnen Ihre privaten Daten entlocken wollen ohne Grund! Seien Sie aufmerksam!

Was tun im Netz: Fotos

- **Fotos:**
Sparsam hochladen und verbreiten.
Lagern die Fotos im Ausland, ist die Rechtslage mehr als unklar
- **Fotos anderer:**
nicht ohne Genehmigung machen (Par. 201A StGB, Spannerparagraph)
geschweige denn irgendwohin hochladen
(Par. 33, 23, 22 KunstUrhG)
(Urheberrecht vs. Recht am eigenen Bild)
Fotosammlungen für die Familie durch Passwort schützen
- **Umgebung aufklären**, warum man selber auch nicht möchte daß andere Bilder von einem unkontrolliert verbreiten
- **Jugendliche aufklären:** es geht auch um Strafbarkeit, nicht nur um den erhobenen Zeigefinger.
- **Sportvereine:** besonders Kinder sind hier samt Bild sehr gut auffindbar!

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

16

Wie erwähnt werden Fotos auch von Stellen, an die man spontan nicht denkt, verwertet. Man denkt immer „ich stell das doch nur für Familie und Freunde ein“, aber es gilt immer: es ist für das GANZE Internet sichtbar.

Wenn man fotografiert und hochladen will, muß man seine menschlichen Motive FRAGEN! Hier geht es auch nicht nur um guten Geschmack, Höflichkeit und erhobenen Zeigefinger, sondern eben auch um Strafrecht.

Suchtfalle: natürlich gefällt es jedem wenn er/sie likes für ein schönes foto bekommt! Ich selber habe dies auch beim Internetdating erfahren, und ich war NIE ein Model ;-)

Was tun im Netz: Familie

- **Familie:**
Familienrechner gehören in den öffentlichen Bereich
- Rechner und Smartphones/Tablets übernachten NICHT im Kinderzimmer
- Keine gute Idee: **Jugendschutzfilter**
man kann soziale Probleme nicht mit Technik lösen!
- Von Kindern lernen: lassen Sie sich das Smartphone erklären.
- **Disziplin:** beim Essen ist für alle das Smartphone tabu

Kinder und Jugendliche wachsen mit Internet und Smartphone als selbstverständliche Technik auf. Dies bedeutet aber nicht, daß in diesem Bereich keine Erziehung stattfinden muss/darf.

Nicht begeistert bin ich von sog. Jugendschutzfiltern. Sie bestehen aus Listen von „verbotenen“ URLs (Adressen) verschiedener Kategorien und müssen ständig aktualisiert werden. D.h.: zuweilen wird zu wenig weggefiltert, weil vom Hersteller noch nicht erkannt oder es wird harmlos falsch positiv erkannt und weggefiltert. Spätestens, wenn man im Versandhandel die **Unterwäscheseiten nicht mehr ansehen kann**, läuft etwas schief.

Außerdem: wollen wir Kinder zu Demokraten erziehen, können wir sie nicht mit Zensurtechnik vertraut aufwachsen lassen!

Kurz: die **Eltern haben die Aufsichtspflicht** und müssen hinsehen und auch Inhalte mit den Kindern diskutieren.

Auch: man MUSS nicht alles ansehen, was einen gruselt oder ekelt.

Was tun im Netz: Mail

- Mailanbieter **in Deutschland** nutzen: GMX, web.de, posteo.de (kostenpflichtig, aber besonders datensparsam!)
- **Mehrere Mailadressen** für Familie/Freunde, Newsletter/Bestellungen
- Diese in verschiedene Ordner sortieren lassen vom Mailprogramm oder der Weboberfläche
- Am besten natürlich: **Mails verschlüsseln!**
=> dies auf der Cryptoparty lernen

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

18

Bei Mails, die auf **Servern liegen, die im Ausland betrieben werden**, wissen wir nicht, wer und welche Dienste darauf zugreifen kann. Die Terrorgefahr treibt diese Dienste aber zu immer ausufernderen Aktionen und späht alles aus, was nicht bei „drei“ auf dem Baum ist.

Ganz praktische Anwendung: **Adressen für Familie und Bestellkrams trennen** und in verschiedene Postfächer sortieren. Dies hat auch den vorteil, daß man u.U. mitbekommt, wenn ein Händler meine Adresse weiterverkauft hat (ich baue gern mal Schreibfehler in meinen Namen ein, das bietet sich ja an).

Beim **Ende-zu-Ende-verschlüsseln von Mail** ergibt sich natürlich das Problem, daß alle Kommunikationspartner hier mitmachen müssen, von einer Seite aus geht es nicht (Details auf der Cryptoparty).

Aber überlegen Sie: an wieviel haben wir uns hier in Deutschland schon gewöhnt/umgewöhnt? **Wir schließen unsere Haustüren ab**, ohne über den Aufwand für die Sicherheit nachzudenken und **wir sortieren den Müll**, weil man uns gesagt hat, daß dies sinnvoll sei.

Was tun im Netz: surfen

- **Privates** Browserfenster nutzen
- **Alternative Suchmaschinen:** duckduckgo, startpage.com
- **Cookies:** Browser so einstellen, daß alle Cookies nach Beenden des Browsers verworfen werden
- **Cache** auch mal löschen
- **Keine Passworte speichern!**
- Komplette anonym surfen: tor-Browser
=> **auch hier: Laptop mitbringen zur Cryptoparty!**

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

19

Im **privaten Browserfenster** speichert der Browser keine Eingaben mit. Jemand, der sich nachher also Zugang zum Rechner verschafft, hat also **keinen Zugriff auf den Browserverlauf** (History).

Verbindet man sich mit dem Internet, bekommt man idR. eine **dynamische IP-Adresse** zugewiesen. Anders als bei einer Telefonnummer ist man über diese also erstmal NICHT identifizierbar. Der Anbieter einer Webseite arbeitet aber gern mit **Cookies**, um einen Besucher beim nächsten Besuch wiederzuerkennen. Bei **Bestellvorgängen** sind Cookies sogar nötig, damit der Warenkorb und der ganze Bestellvorgang nicht in einen undefinierten Zustand kommt, wenn z.B. die Verbindung abbricht. Beim sonstigen Surfen sind sie nicht zwingend nötig und können bei **Beendigung des Browsers** spätestens gelöscht werden.

Um dem Marktführer google nicht zuviele Daten in die Hände zu spielen, kann man andere Suchmaschinen benutzen. Nicht googlen, sondern jetzt: **„enten“!** :)

Auch keine gute Idee ist es, seine sämtlichen Passwörter im Browser (egal ob Rechner/Laptop oder Smartphone) zu speichern. Geht ein Gerät verloren und das Zugangspasswort ist schwach, marodiert der „Finder“ durch sämtliche Bestellplattformen und social Media. Besser man wählt ein gutes Passwortsystem oder nutzt einen Passworttresor wie keepassx.

Einschub: gute Passworte

- FidE,sdFaLg.
Bekannt?
- Gute Passworte bestehen aus den Anfangsbuchstaben von Lieblingsliedern und Gedichten
- Ergänzt um 1-2 Buchstaben von oder hinten pro Anbieter (GX für GMX? Az für Amazon?)
- Ziffern: „ein“ zu „1“ oder englisch „to“, „too“, „two“ zu 2...
- Sonderzeichen: Punkt, Komma, Ausrufezeichen, Dollar, KEINE deutschen Umlaute!

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

20

FidE,sdFaLg.

„Festgemauert in der Erden, steht die Form aus Lehm gebrannt.“
(Die Glocke)

So könnte ein Grundkonzept für ein Passwort aussehen, ergänzt um 1-2 Buchstaben pro Plattform, also z.B.

AzFidE,sdFaLg.

Sie kennen Ihr Lieblingslied und können es sich daher gut merken, für andere Menschen ist es Buchstabensalat.

Bei Sonderzeichen sollte man nur diejenigen wählen, die auf der deutschen und englischen Tastatur an der gleichen Stelle liegen, die Hände „merken“ sich die Passwort irgendwann!

Deutsche Umlaute sind auch keine gute Idee, wenn man im Urlaub im Internetcafé sitzt. Zudem ist bei einigen Anbietern auch die Codierung unklar, was zu Seiteneffekten beim Login führen kann.

Was tun beim mobilen telefonieren?

- Generell: **wieviele Apps** brauche ich wirklich?
- Muß für die Apps **Internet und GPS** ständig ansein? (Leider ja für Messenger)
- **Alternativen zu whatsapp**: Vortrag Februar 2017 (<http://www.cccs.de/>)
- Alternative zum google-Playstore: **f-droid.org**

Brauche ich den Wetterbericht (außer punktuell mal „Warnwetter“, wenn ich draußen unterwegs bin)? Dieser braucht ständig Internet.

Welche Messenger brauche ich? Einige haben den Vorteil gegenüber SMS, daß die Nachricht verschlüsselt werden kann!

Leben ohne google (s. ein anderer Vortrag von mir): f-droid Store.. hat leider nicht alles, z.B. keine Bahn-App.

Aber auch hier: brauche ich die wirklich? Kann ich nicht auch anders buchen?

Wieviel muss der Arbeitgeber wissen?

- ...die **private Mobilnummer** schonmal nicht!
- **Auch bei Schichtarbeit nicht** (Krankenhaus, Einzelhandel).
Es gibt kein Anrecht darauf, durch den AG erreichbar zu sein, es sei denn dies ist vertraglich vereinbart
- **Bereitschaft:** extra Gerät (Telefon, Laptop)
- **Foto auf der Firmenhomepage bedarf der Zustimmung!**
(auch hier: klar ist es schön, wenn alle Apotheker einer Apotheke auf der Webseite sichtbar sind, aber wozu muss DIE WELT das wissen, wie die aussehen? Die KUNDEN kennen einen schließlich, wer anders braucht das nicht.)

Princess @ Stadtbibliothek Vaihingen, 10.11.2017

22

Durch die Verbreitung von Smartphone „verschwimmen“ die Grenzen zwischen beruflich und privat ohnehin schon sehr, denn auch die dienstlichen Mails sind permanent abrufbar. Inwieweit ist man aber verpflichtet, auf diese auch außerhalb der Arbeitszeit zu reagieren? Gar nicht! Tun Sie dies also nur, wenn es vertraglich geregelt ist und Entlohnung oder Freizeit vereinbart ist als Ausgleich.

Der AG darf NICHT verlangen, daß Sie einem Foto auf der Firmenhomepage zustimmen. Die Zustimmung muss aber zwingend vorliegen, auch wenn Sie dort nicht namentlich erwähnt, aber sichtbar sind.

Nicht zuletzt: sich nicht zum Brot machen

- Lesen Sie

<http://de.webfail.com/ffdts>

- Selbst wenn die Hälfte davon gefaked ist:
Lassen Sie es nicht so weit kommen, daß von Ihnen unfassbar dumme Äußerungen im Netz stehen.....

Einladung zu Veranstaltungen

- **Vortragsreihe** des CCCS, 2. Donnerstag im Monat in der Stadtbibliothek am Mailänder Platz:
14.12.2017, 19:30: LFDI Dr. Stefan Brink, „Drei Arten von Datenkraken – Staat, Unternehmen ... und der brave Bürger“
- **Cryptoparties**, ebenfalls Stadtbibliothek am Mailänder Platz, 14-18 Uhr:
3. Februar, 16. Juni, 29. September, 17. November 2018

Kommen Sie und informieren Sie sich!

Fragen / Diskussion

