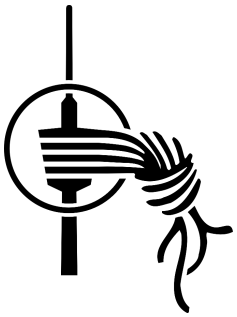


Andrea 'Princess' Wardzichowski

Chaos Computer Club Stuttgart e.V.

http://www.cccs.de/

princess@bofh.de

.

**"Unterm Radar -
wie man sich im Netz bewegt ohne
physikalisch aufgefunden zu werden"**

Frauen helfen Frauen e.V. 14.4.2015

Es ist mir eine echte Freude, heute hierzusein und ich fühle mich durch die Einladung sehr geehrt.

Kurz vorweg: **hat mich jemand gegoogelt?**

Über den CCCS / über mich

Über den CCCS:

- Seit Sommer 2001 Treffen
- Seit Oktober 2003/4 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, Vorträge bei der Informatica Feminale HS Furtwangen 2013, DiB Tagung Uni Stuttgart 2013

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.

Desweiteren pflege ich selber eine gewisse Paranoia und man findet hoffentlich nur wenige Bilder im Netz, dafür aber meine Veröffentlichungen, nicht jedoch Telefonnummern und meine Wohnadresse.

Agenda

- Datenschutz / Datensparsamkeit
- Daten im Browser
- Daten im Smartphone
- Daten in Fotos
- Social Hacking
- Was ist zu tun?
- (praktische Übung: Firefox einstellen)

Viele der hier gegebenen Tips beziehen sich nicht nur auf bedrohte Frauen, vielmehr entsprechen sie Menschen, die auf informationeller Selbstbestimmung bestehen und diese auch durchsetzen wollen.

Datenschutz / Datensparsamkeit

- Immerhin leben wir in Deutschland:
  es gibt das Bundesdatenschutzgesetz (BDSG)
- Allerdings werden auch damit in einem normalen Leben recht viele Daten gespeichert (Einwohnermeldeamt, Bank, Telekommunikation)
- **Eigenverantwortung** bei aktiver Teilnahme am Internet!

Immer mehr Daten werden automatisiert durch (vernetzte) Rechner verarbeitet. Dies erleichtert vieles, eröffnet aber auch die Möglichkeiten, daß Unbefugte Zugang zu Daten erhalten oder sie sogar entwenden können. Dies war mit einem Aktenkeller voller Ordner früher sehr viel schwieriger.

Bei allen Arten von öffentlichen Stellen und Händlern aber gilt das Bundesdatenschutzgesetz. Dies regelt sehr streng mit Zweckbindung und Datensparsamkeit, welche Daten gespeichert und verarbeitet werden dürfen.

Bis auf menschliches Versagen ist man hier grundsätzlich also geschützt.

Anders hingegen verhält es sich mit Daten, die wir selber über uns preisgeben, z.B. über Social Media, Blogs, Foren und Fotosammlungen. Was man selber veröffentlicht, darf gesichtet und verwendet werden. Es verläßt das Netz nie wieder.

Hier kann auch der Gesetzgeber idR. nicht eingreifen.

Informationelle Selbstbestimmung

- ...die fängt eigentlich in der Vergangenheit an :/
- **Öffentliche Stellen, Händler:**
  Datenkorrekturen möglich
- **Internet:** so gut wie unmöglich!
  Betrifft nicht nur Texte, sondern auch Fotos, insbesondere auch Fotos, die andere veröffentlicht haben!

Nutzt man das Internet als reines Informationsmedium und veröffentlicht nichts, ist man auf der **relativ** sicheren Seite. Niemand ist schließlich verpflichtet, sich bei Social Media Plattformen anzumelden.

Ein Problem stellen aber zum Beispiel ungefragt gemachte Fotos dar, die oft ebenso ungefragt veröffentlicht werden. Dabei ist dies in Par. 201A StGB bereits seit 2004 strafbewehrt (bis zu einem Jahr Freiheitsstrafe oder Geldstrafe).

Schwierig ist hier sehr oft die Sensibilisierung des sozialen Umfeldes.

Daten im Browser / wenn der Laptop abhanden kommt / Daten auf dem heimischen Rechner

- Bookmarks (Favoriten, Lesezeichen)
- Eingabe-Historie in der Adresszeile
- Eingabe-Historie in ausfüllbaren Feldern geben u.U. Aufschluß auf den Aufenthaltsort
  (Routenplaner, www.vvs.de)
- Abgespeicherte Passworte geben Zugriff auf soziale Netzwerke und Versandhändler
- Alle Daten/Cookies beim Beenden löschen lassen
- „Private Window“ verwenden, dann wird nichts gespeichert
- Alle Passworte ändern, wenn ein Rechner mit gespeicherten Passworten zurückgelassen werden musste.

Unverzichtbar beim Umgang mit dem Internet ist der Browser. Erst mit seiner Erfindung wurde das Internet für jedermann zugänglich. Vorher waren für jeden Dienst einzelne Programme zu erlernen, zumeist ohne graphische Benutzeroberfläche.

Was das Bedienen des Browsers komfortabel und einfach macht, ist aber gleichzeitig eine Datensammlung, die Rückschlüsse auf sehr vieles zuläßt.

Daher sollte eingestellt werden, daß Eingaben und Cookies beim Beenden des Browsers verworfen werden. Dies erreicht man auch, wenn man den Speicher (Cache) während der Sitzung manuell löscht oder wenn man ohnehin ein „private Window“ nutzt.

Im Browser abgespeicherte Passworte sorgen zudem dafür, daß jemand mit Zugriff auf den Rechner z.B. auch Bestellvorgänge tätigen kann, ebenso wie Mails lesen und versenden und an sozialen Netzwerken teilnehmen. Passworte sollten also nie abgespeichert werden. Damit man sie sich gut merken kann, nimmt man die Anfangsbuchstaben von Gedicht- und Liedzeilen und fügt je nach Anbieter/Plattform ein bis zwei Buchstaben vorn oder hinten an. So wird auch vermieden, daß nur ein einziges Passwort existiert. Nicht geeignet als Passworte sind alle Worte, die sich in einem Lexikon befinden.

Daten im Smartphone

- Gerät immer sichern (Pin >= 5 Stellen, automatisches Sperren einschalten)
- Wenn möglich Speicher verschlüsseln
- Backup bei Android: Daten liegen bei google :/
- GPS ausschalten
- WLAN-Ortung ausschalten (Standort kann auch anhand der verfügbaren WLANs ermittelt werden)
- **=> Flugmodus**
- Nicht benötigte Apps deinstallieren / deaktivieren
- Berechtigungen der Apps prüfen!

Bei einem Smartphone kommen zu den Browserdaten Aufenthaltskoordinaten hinzu. Für Navigation und viele Services (und sei es nur der Pizzadienst) wird GPS benötigt. Ebenso kann der Standort anhand von verfügbaren WLANs ermittelt werden.

Gut: diese Daten liegen nur dem Mobilfunkanbieter vor, dieser kann aber durch Social Hacking getäuscht werden!

Generell gilt aber auch: Smartphone sichern (kann leichter verlorengehen als ein größerer Rechner), sparsam mit der Installation von Apps sein, diese auf ihre Rechte prüfen.

Herkömmliche Mobiltelefone

- Viel geringere Risiken
- Kein GPS, WLAN
- Anbieter hat nach wie vor alle Daten
- Anonyme Mobilfunkverträge in .de nicht möglich
- Idee: Supermarkt-Karte mit valider, aber nicht echter Adresse kaufen und auch nur an der Kasse (nicht über ein Konto) aufladen (am Rande der Legalität....)

Bei herkömmlichen Mobiltelefonen hat der Anbieter nur die Funkzelle, die gern auch mal einen ganzen Stadtteil umfassen kann. Das Aufspüren einer Person ist hier ungleich schwieriger.

Für das Aufrechterhalten der Kommunikation mit wichtigen Kontaktpersonen aber reichen Telefonie und SMS eigentlich aus.

Zudem werden keine Daten und Inhalte auf Servern außerhalb Deutschlands gespeichert (whatsapp).

Wie schnell komme ich an eine neue Mobilfunknummer?

Anbieter	Reaktionszeit	Bemerkung	Dauer	Kosten
eplus	1 Stunde	Und das nachts!	24-48 h	15 Euro
Vodafone	1,5 Tage	Keine Infos per Mail, wollen erstmal meine Daten. War dann im Shop.	sofort	20 Euro
T-Mobile	Keinerlei Reaktion	War dann im Shop	10 Minuten	25 Euro
O2	Knapp 2 Tage	Quengeln auch dass sie keine Daten von mir haben, geben dann aber Auskunft	Innerhalb 24h SMS mit neuer Nummer	29,99 Euro

Im Zuge der Vorbereitung dieses Vortrags ging mir diese Fragestellung durch den Kopf, denn Telefonklingeln und SMS ist leider sehr viel invasiver und lästiger als unerwünschte E-Mails. Diese lassen sich sehr leicht filtern. Daher ist vielleicht ein Aspekt, sich eine neue Nummer zuzulegen. Oft ist man mit Verträgen auch gebunden und möchte diese auch aus finanziellen Gründen nicht zugunsten einer Prepaid-Karte brachliegen lassen. Das Ändern der Rufnummer und kontrolliertes Herausgeben der neuen Nummer kann also ein Teil des Vorgehens sein.

Aber auch hier gilt: man muß sein Umfeld dahingehend sensibilisieren, daß es die neue Nummer auch nicht ungefragt an Dritte herausgibt, sondern sagt „Gib Du mir Deine Kontakdaten, ich leite diese weiter und sie/er wird sich dann bei Dir melden“.

Daten in Fotos

- Fotos, die mit Smartphones und Digitalkameras erstellt werden, enthalten Metadaten, sog. **Exif-Daten**
- Datum, Uhrzeit, Orientierung (Bilddrehung), Belichtung, Brennweite (uvam.), Kameramodell, aber auch **GPS-Koordinaten**
- Wird ein solches Bild verschickt oder hochgeladen, kann diese Information ausgelesen werden
- Ansehen/bearbeiten unter Windows mit:
  Exif-Viewer (bei chip.de ladbar), exifread (PC-Welt), ExifTool (Heise.de)
- Generell: unkontrolliertes Fotografieren-lassen unterbinden.

Während bei Internet- und Mobilfunkanbietern zuerst einmal nur der Anbieter Zugriff auf Verbindungs- und Standortdaten hat, sind veröffentlichte Fotos für jedermann zugänglich. Enthalten diese in den Exif-Daten Geokoordinaten, kann man den Aufenthaltsort einer Person recht gut ermitteln. Ich persönlich halte daher Fotos für die heikelsten Daten, da jeder auf sie Zugriff haben kann. Auf Verbindungsdaten von Mobilfunkanbietern erhalten idR. nur Polizei und Staatsanwaltschaft Zugriff.

Social Hacking

- Problem: Sachbearbeiter / Hotlinemitarbeiter WOLLEN helfen
- Menschliches Verhalten kann aber zu Datenschutzverstößen führen
- Auch: Unkenntnis, Sorglosigkeit auch bei offiziellen Stellen

In der Trilogie „Verblendung“ von Stieg Larsson ist die Hauptperson neben dem Journalisten eine junge, leicht autistische Hackerin. Sie verschafft sich nicht nur technisch Zugang zu Daten, sondern auch durch geschicktes Ausfragen von (Amts-)Personen.

Dieser Vorgang wird als Social Hacking oder Social Engeneering bezeichnet. Es wird Redseeligkeit ausgenutzt, ebenso wie die Tatsache, daß Hotlinemitarbeiter ja ihren Kunden gerne helfen **wollen**. Oft werden dabei dann Sicherheitsmaßnahmen, die Kunden und Daten schützen sollen, dann zugunsten der Hilfe und Erledigung eines Problems umgangen.

Angriffsvektoren: wo liegen die Daten und gegen wen müssen wir uns schützen?

- Anbieter (Social Media, Telefon) hat immer alle Daten, darf diese idR. aber nicht herausgeben (außer an Ermittlungsbehörden)
- Laptop wurde geklaut s.o.
- Rechner im gemeinsamen Haushalt hat alle Passworte gespeichert
- Hersteller-“Feature“: Ortungssystem bei Laptop-Klau (s. Social Hacking, hier hilft TAILS, s.u.)
- Smartphone/Handy: Betreiber hat alle Infos, darf sie aber nicht herausgeben (aber auch hier: Social Hacking möglich)
- „Handy verloren“ -> Ortungssysteme
- GPS-Daten in Fotos: für jedermann einsehbar, wenn Fotos irgendwo veröffentlicht sind
- Aktive Teilnahme an Social Media einstellen. Beabsichtigt und unbeabsichtigt wird zuviel preisgeben, auch im nicht-bedrohten Zustand.

Wie erwähnt kommt man als normaler Mensch an Daten von Internet und Telefonanbietern schwer heran. Leichter hingegen ist es, die Ortungsfunktionen gegen Diebstahl zu aktivieren. Dies kann sehr wahrscheinlich auch ein Ehepartner anstoßen, wodurch eine bedrohte Frau auffindbar wird. Es sollte daher abgefragt werden, ob zu mitgebrachten Geräten eine solche Diebstahlsicherung existiert. Wenn ja, dürfen diese nicht in Betrieb genommen werden.

Ob eine SIM-Karte bei Eintritt in die anonyme Wohnung zerstört werden muß, ist nicht sicher. Es könnte schon helfen, die Rufnummer zu ändern. Ein Problem stellen dann aber noch Papierrechnungen dar, die in der gemeinsamen Wohnung zurückgelassen wurden, denn sie enthalten die Vertragsnummer, mit der (wieder social hacking) Vertragsdetails erfragt werden können.

Idee: Mobilfunkanbieter anfragen, wie in solchen Fällen verhindert werden kann, daß Anruflisten oder neue Nummern herausgegeben werden.

Unterm Radar – was ist zu tun?

- man muß sich nicht überall mit seinem richtigen Namen anmelden
- keine Adress- Telefon- Kontodaten ohne Not preisgeben
  ohnehin nicht alle Formulare ohne Nachdenken ausfüllen
- Adresssperre beim Einwohnermeldeamt (einfache Form geht immer!)
- Mail, Webseiten, Blogs bei deutschen Anbietern hosten
- Mails verschlüsseln!
- Sparsam mit Fotos sein, auch Freunde/Familie darauf hinweisen, Fotosammlungen mit Passwort schützen
- Möglichst nur in .de bestellen, nicht im Ausland
- sich gegen Datenkraken wehren! Nachfragen! Welche Daten sind gespeichert und wie lange (Auskunft muß einmal im Jahr unentgeltlich gegeben werden, auch die Schufa!)
- Auch: öffentliche Stellen anfragen (SSB, Videoüberwachung)

Diese Hinweise gelten eigentlich für jeden, nicht nur für bedrohte Frauen. Wir hier in Deutschland sind gerade beim Formulare ausfüllen sehr ordentlich! Man darf aber auch einmal Felder unausgefüllt lassen. In Webmasken werden Eingaben manchmal erzwungen, meist bei Telefonnummern. Hier gibt man dann wirklich 12345678 ein.

Nur Inhalte, die bei deutschen Anbietern liegen, unterliegen auch dem deutschen Datenschutzgesetz. Anbieter im Ausland nicht oder es ist nur sehr schwer durchzusetzen.

Absurdes Beispiel: facebook speichert unendlich viele Daten (auch was man eigentlich „gelöscht“ hat), gibt aber nichts davon an deutsche Ermittlungsbehörden heraus.

Juristische Fallstricke drohen auch beim Bestellen im Ausland: sollte etwas nicht funktionieren ist es sehr schwer, sein Recht auch durchzusetzen.

Mails zu verschlüsseln macht auf den ersten Blick Aufwand, aber diesen treiben wir auch täglich und schließen Wohnung und Auto ab, ebenso wie wir versuchen Müll zu trennen und Energie nicht zu verschwenden. In der Summe erzielt dies dann schon Effekte!

Smartphone mit „wenig google“ (nur Android, nicht iPhone)

- Firefox Browser statt eingebautem Browser
- Alternative Suchmaschinen: https://startpage.com, https://ixquick.de/ (de!), https://duckduckgo.com/
- Mailprogramm K9 statt googlemail
- Posteo.de statt gmail (gmx.de, web.de)
- Kalender: DAVdroid und owncloud statt google Kalender
- Scout / OpenStreetMap statt google maps

Nicht zu unterschätzen sind aber auch unternehmensmaßige Datensammler wie google. Aber auch hier gibt es Alternativen! Probieren Sie es aus!

Mailkonten bei posteo.de kosten zwar etwas (1 Euro im Monat), es werden aber keine persönlichen Daten abgefragt. Das sollte es einem schon Wert sein. Ebenso empfehle ich, mehrere Mailadressen für Privates und Bestellvorgänge sowie Newsletter zu verwenden.

Sicher ins Internet

- TAILS (von CD oder USB Stick booten) http://tails.boum.org/
- Stadtbibliothek (mit dem Büchereiausweis können Laptops entliehen werden, die nach Benutzung komplett gelöscht werden)
- Sonst: nicht an fremden Rechnern Passworte eingeben (Keylogger!)

Befindet man sich in einer Umgebung, in der man keinen eigenen Rechner zur Verfügung hat, ist es oft hilfreich einen Rechner von CD mit einer sicheren Umgebung zu booten. So geht man auch vor, wenn man einen Rechner auf Virenbefall testen möchte, dies ist also unter IT'lern ein normales Verfahren.

Für TAILS gibt es Anleitungen im Netz und ich habe einige DVDs zum ausprobieren mitgebracht.

Generell gilt: an fremden Rechnern möglichst keine Passworte eingeben und schon gar nicht im Browser abspeichern.

Praktische Übung: Firefox

- https://cryptopartystadtbib.piratenpad.de/linksammlung?
- Nützliche Addons: adblock edge, flashblock, https everywhere, disconnect
- Unnötige Plugins/Addons deinstallieren
- Bearbeiten -> Einstellungen

Danksagungen

- Thomas Waldmann (surfen)
- Stefan Leibfarth (Smartphones)

Tips / Linksammlung / Cryptoparty

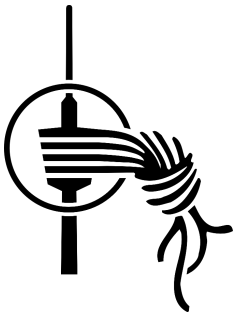
https://cryptopartystadtbib.piratenpad.de/linksammlung ?

Emails verschlüsseln mit Thunderbird und enigmail:
https://emailselfdefense.fsf.org/de/

Nächste Cryptoparty in der Stadtbibliothek am Mailänder Platz:
27. Juni 2015, 13-17 Uhr

Regelmäßige Vorträge: idR. 2. Donnerstag im Monat, Stadtbibliothek

Fragen und Diskussion



?

?

?