Wie Journalisten sicher im Netz arbeiten

# Verschleiern – Verschlüsseln – Verstecken


Mainz, 21. November 2009

Albrecht Ude

Schutz der eigenen Daten und der eigenen Kommunikation – insbesondere der Informantenschutz – ist eine journalistische Kernaufgabe, die nicht delegiert werden kann, da dies bereits einen Bruch der Vertraulichkeit bedeutete.

**Überwachung = Angriff!**

# Die "eiserne" Faustregel der Überwachung

Was an Überwachungsmaßnahmen technisch möglich und finanzierbar ist, das geschieht auch.

Im Internet bedeutet dies die Möglichkeit zur totalen Überwachung.

Die üblichen Hebel: Terrorismus, Kinderpornographie und Geldfälschung

Technische Maßnahmen sind nicht hinreichend, um das Problem, dass die Überwachung für eine freie, demokratische Gesellschaft darstellt, zu lösen. Nötig sind politische Massnahmen, die Überwachung begrenzen und wirkungsvoll kontrollieren.

# 1. Paradox

Wir recherchieren ...

... müssen uns aber davor schützen, selbst recherchiert zu werden.

Die Bedrohungslage von Journalisten und Redaktionen ist relativ homogen:

- Die "Geschäftsgeheimnisse" sind immateriell
- Die "Geschäftsgeheimnisse" sind substanziell
- Die normale Redaktion ist ein offenes Haus

**Überwachung = Angriff!**

# Was wird überwacht?

1. Datenbestände = eigener Rechner | eigenes Netz

   Online-Durchsuchung
   Schadsoftware (z.B. Tauschbörsen)

2. Kommunikationsinhalte

   Welche Nachrichten werden weitergegeben?
   Welche Websites werden angesurft?

3. Verkehrsdaten

   s.g. "Vorratsdatenspeicherung"
   Wer kommuniziert mit wem?
   Wer hat zu wem Kontakt?

Das sieht z.B. so aus:


Quelle: Verfassungsschutz BW

# Wer überwacht | greift an?

1. Der Staat | die Staaten

   Polizei | Staatsanwaltschaft | Zoll ...
   Geheimdienste (Deutschland, USA, Kasachstan)

2. Die Wirtschaft

   Datensammler wie Google
   Firmen mit (Des-)Interesse an Berichterstattung
   Die Provider (im Staatsauftrag)

3. Interessierte Dritte

   Skript Kiddies, Hacker, Bot-Netze

# Überwachungsgeräte (1)

Moderne Kopierer

- haben Festplatten
- haben Netzwerkanschlüsse
- Bringen Codierungen auf jedem Farbausdruck an

Moderne Drucker

- sind via E-Mail ansprechbar
- haben Netzwerkanschlüsse
- Bringen Codierungen auf jedem Farbausdruck an

http://w2.eff.org/Privacy/printers/docucolor/index.php

# 2. Paradox

Der Staat will unsere Daten, muss aber Datensicherheit garantieren.

Eine gute Richtschnur bietet die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in derInformationstechnologie (BSI), z.B. der G 5 Gefährdungskatalog "Vorsätzliche Handlungen".

BSI: IT-Grundschutz-Kataloge:

**https://www.bsi.bund.de/cln_134/DE/Themen/ITGrundschutz/itgrundschutz_node.html**

BSI: G 5 – Gefährdungskatalog Vorsätzliche Handlungen:

**https://www.bsi.bund.de/cln_134/ContentBSI/grundschutz/kataloge/g/g05/g05.html**

# Überwachungsgeräte (2)

alt (2000)

Keystroke-Logger (physikalisch)

neu (2008)


Keystroke-Logger (virtuell)

# Was tun?

1.) eigenen Rechner sichern

2.) Verschleiern: Anonymsieren

3.) Verschlüsseln : Kryptographie

4.) Verstecken : Steganographie

# 1.) eigenen Rechner sichern

Schutz vor Zugriff via Netz (z.B.Online-Durchsuchung)

"Tatsächlich sind keine Möglichkeiten bekannt, eine Online-Durchsuchung so zu gestalten, dass ein Zielsystem nicht wirksam davor geschützt werden kann."

Stellungnahme zur "Online-Durchsuchung" - Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07 / von Dirk Fox, Secorvo Security Consulting GmbH

Version 1.1, Stand 29. September 2007

http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf

# 1.) eigenen Rechner sichern

Dirk Fox, BVerfG-Stellungnahme, 4.2 :
Verhinderung der Installation der Durchsuchungssoftware

1.) Patchen des Betriebssystems
2.) Restriktive Konfiguration des Systems
3.) Restriktive Konfiguration des Browsers
4.) Nutzung eines Virenscanners
5.) Sicherheitssensibler Umgang mit E-Mails
6.) Nutzung einer Personal Firewall
7.) Einsatz "Virtueller Maschinen"

# 1.) eigenen Rechner sichern

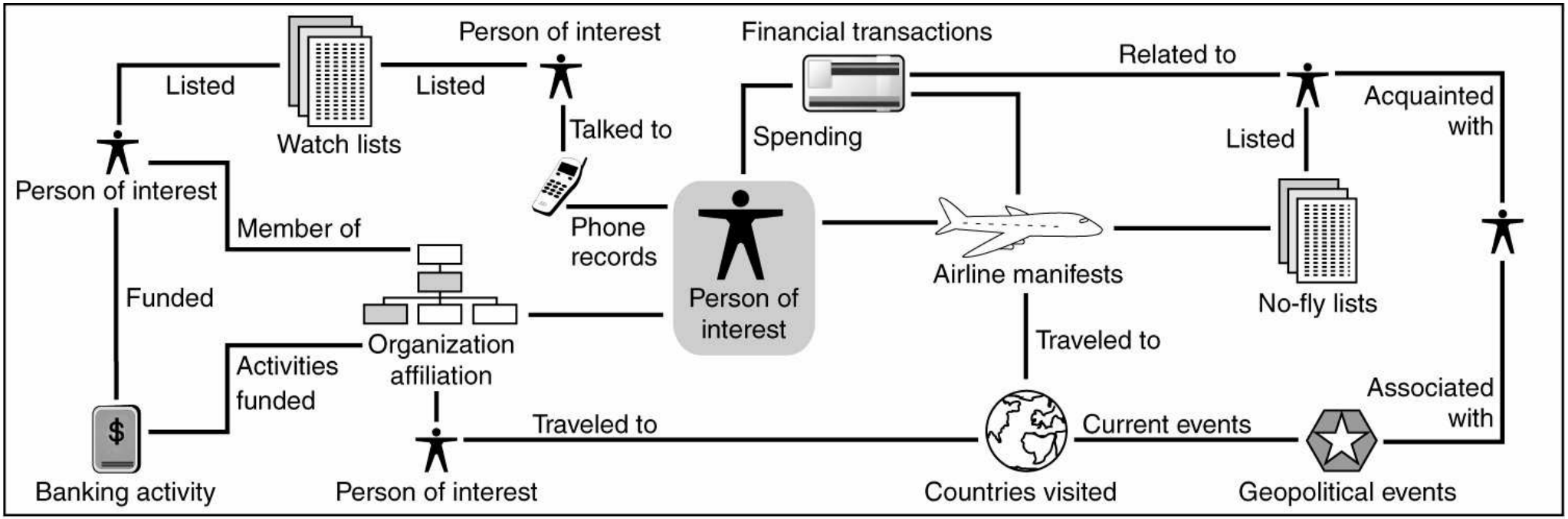
Firefox-Erweiterungen für sicheres und ungestörtes Surfen

NoScript : Konfiguration der Javascripts für die jeweilige Website
FoxyProxy : Einrichtung mehrerer Proxy-Profile
Adblock Plus : Werbeblocker
CookieSafe : Konfiguration der Cookies für die jeweilige Website.
Flashblock : Konfiguration der Flash-Animationen für die jeweilige Website.
Layerblock : Konfiguration von Layer-Fenstern für die jeweilige Website.
RefControl : Manipulation des eigenen Referer-Headers
Cache Status : Konfiguration (und selektive Löschung) des eigenen Cache.
SafeCache : Gegen Tracking (unbemerktes Auslesen) des Caches.
SafeHistory : Gegen Tracking (unbemerktes Auslesen) der History.

... es gibt noch mehr davon - s. Linkliste.

# 2.) Verschleiern: Anonymsieren

## Anonymisierung verschleiert Verkehrsdaten




Source: GAO.

# 2.) Verschleiern: Anonymsieren

Anfangs-Anonymisierung

- Keine Spuren auf dem Rechner, an dem man arbeitet (sehr schwierig!)
- Keine Hinweise, wem eine E-Mail geschickt wurde

Internet-Cafe (Achtung KeyLogger!)
nur den eigenen - abgesicherten - Rechner nutzen

End-Anonymisierung

- Keine (korrekten) Hinweise auf den Seite, die man ansurft
- Keine Hinweise, wer eine E-Mail geschickt hat

Caches, Proxies, TOR, Remailer, Privacybox

# 2.) Verschleiern: Anonymsieren

Es fließen mehr Daten, als man denkt!

Testseiten von Privacy.net und Leader.ru zeigen, welche Informationen über Ihren Rechner an Webauftritte übergeben werden bzw. von diesen abgefragt werden können.

(Achtung: Eine gut konfigurierte Firewall sollte während dieses Tests mehrmals Alarm geben.)

Beispiel:
Was der Besitzer einer angesurften Webseite erfährt
http://www.leader.ru/secure/who.html

# 2.) Verschleiern: Anonymsieren

Caches

Es gibt viele Zwischenspeicher ("Cache") im Netz, die öffentlich zugänglich sind. Wer diese nutzt, bleibt unentdeckt.

Wichtig: Jede Seite muss einzeln aus dem Cache aufgerufen werden.

Caches rufen tw. Grafiken von der Originalseite ab!

- Ask, Bing, Google, Yahoo
  http://www.google.com/ http://www.ask.com/
  http://search.yahoo.com/ http://search.live.com/
- Faganfinder URLinfo
  http://www.faganfinder.com/urlinfo/

# 2.) Verschleiern: Anonymsieren

Proxies

Proxy-Server surfen im Auftrag des Nutzers, verschleiern dessen IP-Adresse.

Wichtig: Cookies, Session-IDs, Logins usw. brechen die Anonymität.

- TOR ("The Onion Router"), I2P, JAP
  https://www.torproject.org/
- PrivacyDongle: Anonymität für die Westentasche
  http://www.privacydongle.de/
- Offene Proxies
  Google: inurl:proxy.cgi
  http://www.google.com/search?hl=en&q=inurl%3Aproxy.cgi&btnG=Search

# 2.) Verschleiern: Anonymsieren

Remailer

Remailer verschleiern den Weg und den Absender einer E-Mail

- Anon-E-Mail
  Anonyme E-Mails an frei wählbare Empfänger (Mixmaster-Interface)
  https://www.awxcnx.de/anon-email.htm
- Mixmaster
  http://mixmaster.sourceforge.net/
- Privacy-Box (PGP-Nutzung ohne Installation!)
  Anonyme E-Mails an bestimmte, pseudonymisierte Empfänger
  optional unter Nutzung von deren PGP-Keys
  https://privacybox.de/

# 3.) Verschlüsseln: Kryptographie

Dateien, Verzeichnisse, Partitionen, Speichermedien verschlüsseln

- Truecrypt
  http://www.truecrypt.org/

Dateien und E-Mails verschlüsseln

Problem: Alle Kommunikationsteilnehmer müssen Programme installieren und Schlüssel austauschen

- PGP
  http://www.pgpi.org/
- GnuPG
  http://www.gnupp.org/start.html

  http://www.gpg4win.org/

# 4.)Verstecken: Steganographie

Steganographie-Programme verstecken Nachrichten in 'unverdächtigen' Dateien, z.B. Bildern.

Truecrypt

Das Programm hat eine starke Steganographe-Komponente

Dateien / Verzeichnisse können in Dateien ('Containern') versteckt werden

Auswahl des Containers über Password

# Hilfreiche Links

## Hintergrundinformationen

Stellungnahme zur "Online-Durchsuchung" - Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07 / von Dirk Fox, Secorvo Security Consulting GmbH
Version 1.1, Stand 29. September 2007
http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf
(PDF-Datei, 17 S., 115 KB)
Sehr lesenswerter Text, der u.a. eine Kurzanleitung zur Absicherung von Rechnern enthält.

Qualifizierter Selbstschutz : 10 Schritte zur Rechnersicherheit / von A. Ude
http://www.ude.de/internet/qualifizierter-selbstschutz-10-schritte-zur-rechnersicherheit.html

Eine gute Richtschnur bietet die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in derInformationstechnologie (BSI), z.B. der G 5 Gefährdungskatalog "Vorsätzliche Handlungen".
BSI: IT-Grundschutz-Kataloge:
http://www.bsi.bund.de/gshb/index.htm
BSI: G 5 – Gefährdungskatalog Vorsätzliche Handlungen:
http://www.bsi.bund.de/gshb/deutsch/g/g05.htm
Die vollständigsten deutschensprachigen Dokumente zum Thema - leider überkomplett. Ausgedruckt umfasst das Grundschutzhandbuch mehrere Aktenordner.

Eine sinnvolle, nicht verkürzende, aber kurze Anleitung für Journalisten und Redaktionen fehlt noch.

Was weiß der Besitzer einer Webseite über uns?
http://www.leader.ru/secure/who.html
Diese Site analysiert, was sie über den Surfer ermitteln kann.

## Erweiterungen (Addons) für den Firefox-Browser für sicheres und ungestörtes Surfen

FoxyProxy
http://foxyproxy.mozdev.org
http://addons.mozilla.org/de/firefox/addon/2464
Ermöglicht die Einrichtung mehrerer Proxy-Profile, zwischen denen im laufenden Betrieb gewechselt werden kann.

Adblock Plus
http://adblockplus.org
http://addons.mozilla.org/de/firefox/addon/1865
Werbeblocker - technisch gesehen ein Filter für bestimmte (konfigurierbare) Inhalte von Webseiten.

NoScript
http://noscript.net
http://addons.mozilla.org/de/firefox/addon/722
Konfiguration der Javascripts für die jeweilige Website - Sie entscheiden, welches ausgeführt wird.

Controle de Scripts
http://addons.mozilla.org/en-US/firefox/addon/1154
Bessere Kontrolle der Javascript-Optionen.

CookieSafe
http://forum.softwareblaze.com
http://addons.mozilla.org/de/firefox/addon/2497
Konfiguration der Cookies für die jeweilige Website.

Fasterfox
http://fasterfox.mozdev.org
http://addons.mozilla.org/en-US/firefox/addon/1269
Schneller Aufbau von Webseiten im Browser durch Zu- / Abschalten bestimmter Funktionen

Flashblock
http://flashblock.mozdev.org
http://addons.mozilla.org/en-US/firefox/addon/433
Konfiguration der Flash-Animationen für die jeweilige Website.

Layerblock
http://home.arcor.de/jonha/lb
Konfiguration von Layer-Fenstern für die jeweilige Website.

RefControl
http://www.stardrifter.org/refcontrol
Zur Manipulation des Referer Headers, den der eigene Browser an einen Webserver übermittelt.

Cache Status
http://addons.mozilla.org/de/firefox/addon/1881
Konfiguration (und selektive Löschung) des eigenen Cache.

SafeCache
http://www.safecache.com
http://addons.mozilla.org/de/firefox/addon/1474
Gegen Tracking (unbemerktes Auslesen) des Caches.

SafeHistory
http://www.safehistory.com
http://addons.mozilla.org/de/firefox/addon/1502
Gegen Tracking (unbemerktes Auslesen) der History.

Secure Login
http://blueimp.net/mozilla
http://addons.mozilla.org/de/firefox/addon/4429
Verstärkt die Sicherheit des Firefox-eigenen Password-Managers.

TrackMeNot
http://mrl.nyu.edu/~dhowe/TrackMeNot
http://addons.mozilla.org/en-US/firefox/addon/3173
Täuscht Suchanfragen vor, um in Logfiles Verwirrung zu stiften (Spurenverwischung, keine Beseitigung!).

User Agent Switcher
http://chrispederick.com/work/user-agent-switcher
http://addons.mozilla.org/de/firefox/addon/59
Zur Manipulation der an Webserver übermittelten Angabe HTTP_USER_AGENT.

Spoof Stick
http://www.erweiterungen.de/detail/Spoof_Stick
Zum Aufdecken von URL-Spoofing (gefakten Websites).

## Erweiterungen zum anonymen Surfen

TorButton
http://addons.mozilla.org/en-US/firefox/addon/2275
TOR (das Anonymisierungsnetz "The Onion Router") im laufenden Betrieb zu- / ausschalten.

Anonymization Toolbar
http://anonymization.net
http://addons.mozilla.org/en-US/firefox/addon/2217
Toolbar für anonymes Surfen.

Anonymouser
http://addons.mozilla.org/en-US/firefox/addon/1415
Tool zum anonymen Surfen (nicht kompatibel mit derzeit aktueller FF-Version).

Show MyIP
http://addons.mozilla.org/en-US/firefox/addon/4530
Zeigt die eigene, aktuelle IP-Adresse an.

MyIP
http://addons.mozilla.org/en-US/firefox/addon/2521
http://addons.mozilla.org/en-US/firefox/addons/policy/0/2521/13857
Dito.

## Anonymisierung

### Caches
Die Caches der großen Universalsuchmaschinen Google, Yahoo, Ask, Live

Weitere Caches findet man bei Faganfinder
http://www.faganfinder.com/urlinfo/

### Proxies
TOR
https://www.torproject.org/

I2P
http://www.i2p2.de/

JAP
https://www.jondos.de/de/

Offene Proxies findet man leicht z.B. durch eine Google-Recherche (wobei ich hier davon ausgehe, dass viele Proxies "proxy" heissen und die CGI-Schnittstelle nutzen
Google: inurl:proxy.cgi
http://www.google.com/search?hl=en&q=inurl%3Aproxy.cgi&btnG=Search

### Remailer
Anon-E-Mail
Anonyme E-Mails an frei wählbare Empfänger (Mixmaster-Interface)
https://www.awxcnx.de/anon-email.htm

Mixmaster
http://mixmaster.sourceforge.net/

Privacy-Box (PGP-Nutzung ohne Installation!)
Anonyme E-Mails an bestimmte, pseudonymisierte Empfänger
optional unter Nutzung von deren PGP-Keys
https://privacybox.de/

PrivacyDongle
http://www.privacydongle.de/
https://www.foebud.org/datenschutz-buergerrechte/vorratsdatenspeicherung/privacydongle
https://shop.foebud.org/product_info.php?pName=privacydongle-torpark-auf-usbstick-p-151&cName=gadgets-c-26

## Verschlüsselung

Truecrypt
http://www.truecrypt.org/

PGP
http://www.pgpi.org/

GnuPG
http://www.gnupp.org/start.html

GPG for Windows
http://www.gpg4win.org/

**Vielen Dank für die Aufmerksamkeit**

Albrecht Ude
mailto:albrecht@ude.de
http://www.ude.de/