Vorsichtsmassnahmen
im Nach-Snowden-Zeitalter

14. Magglinger Rechtsinformatikseminar 2014

Data Factory AG, 8057 Zürich

PC/Mac

Das Gerät nicht unbeaufsichtigt herumstehen lassen!

Startup-Sicherheit:

- Passwörter setzen
- Fingerabdruck-Erkennung
- Gesichtserkennung
- Hardware-Token (Zertifikat)

Updates des Betriebssystems und der benutzten Programme stets installieren

Antiviren-/Antispyware-Software installieren und stets aktualisieren

- Mac: **Norton Antivirus**, **McAfee VirusScan**, **ProtectMac**, **iAntivirus**, **VirusBarrier X6**, **MacScan**
- Windows: **Norton Antivirus**, **McAfee Antivirus Plus**, **Avast**, **F-Secure**, **Bitdefender**, **Spyware Terminator**

Kamera und Mikrophon abdecken wenn nicht gebraucht

Software zum Löschen aller Cookies (auch Supercookies!) verwenden

- Windows[1]: **Cookie Manager**
- Mac[2]: **BetterPrivacy** (für Firefox)


Verschlüsselung des internen Disks:

- Windows:
  - **Truecrypt**
  - **BitLocker** [Ultimate- oder Enterprise-Version von Windows 7 oder Vista, oder die Pro-, beziehungsweise Enterprise-Version von Windows 8; der PC muss über einen TPM-Chip (Trusted Platform Module) verfügen].
- Mac: FileVault Protection einschalten.

Nicht mehr benötigte Dateien restlos löschen:

- Windows: **PrivaZer**, **Eraser**
- Mac: Wählen Sie im Menü "Finder“ den Menüpunkt "Papierkorb sicher entleeren“.

---

[1] Speicherort: %AppData%\Roaming\Macromedia\Flash Player\#SharedObjects

[2] Speicherort: ~/Library/Preferences/Macromedia/Flash Player/#SharedObjects

Externe Speicher

- Zertifizierte SSD-Hochsicherheitsfestplatte **HS256S** von DIGITTRADE GmbH. Zwei-Faktor-Authentifizierung mittels Smartcard und 8-stelliger PIN.
- USB-Sticks mit Verschlüsselungs-Software. z.B. **SafeToGo** mit Hardware-Verschlüsselung, einfachere Modelle mit Software-Verschlüsselung. 60% aller USB-Sticks gehen verloren. 84% davon werden wieder gefunden. Nur: von wem?
- Vorsicht bei geschenkten oder gefundenen USB-Sticks

Router für WLAN

- Verkehr verschlüsseln mit WPA2
- ev. Zugang beschränken auf bestimmte Mac-Adressen (Media-Access-Control-Adresse)
- sicheres Passwort verwenden (für Admin-Funktion und für WLAN-Zugriff)

Cloud

- Cloud-Zugriff der Apps restriktiv definieren. Besser keine Dienste benützen, die ausserhalb Europas stehen, also nicht Google, Microsoft usw.
- **Dropbox**: nur mit Verschlüsselungssoftware benützen, z.B.
  - **BoxCryptor** (Windows, iOS und Android)
  - **Steganos** Passwort Manager 15 (nur für Windows)
  - **Cloudfogger** (für Windows und Android)
  - **CryptSynch** (Windows, ohne iOS und Android)
- Gute Alternative: **wuala** (Windows, Browser[3], iOS, Android). Die Verschlüsselung erfolgt hier bereits auf dem absendenden Gerät, sodass auch bei Zugriff auf den Server nicht mitgelesen werden kann. Die Server stehen in der Schweiz, in Deutschland und in Frankreich.

Browser

Wenn Sie sich im Internet bewegen, wird üblicherweise jede Ihrer Eingaben registriert und ausgewertet: Welche URLs rufen Sie auf? Wonach suchen Sie? Wonach haben Sie gestern und letzte Woche gesucht? Was lässt sich daraus schliessen? Es werden beispielsweise Angaben gesammelt zu: Alter, Geschlecht, Gewicht, Grösse, Zivilstand, Ausbildung, politische Ausrichtung, Einkaufsgewohnheiten, Haushaltseinkommen, Gesundheitszustand, Ferienpläne. Online-Daten werden mit Offline-Daten kombiniert

[3] setzt Java voraus

Wichtig ist deshalb, Klarheit zu schaffen und Transparenz: Wer holt welche Infos? Dabei helfen folgende Produkte:

- **Epic Browser** (Mozilla-Derivat, für Windows und Mac OS X): statt IE, Opera, Chrome: schnell, zuverlässig, diskret. Registriert keine URLs, löscht nach Beendigung immer alle Cookies, die History und den Cache-Speicher. Fakultativ: Proxy. Bevorzugt SSL-Verbindungen.
- **Startpage** statt Google: transparenter Zugriff auf Google, aber https-Verbindung, kein Tracking, keine Cookies, registriert weder IP-Adresse noch Suchbegriffe, stellt Proxy zur Verfügung
- **TrackerBlock** (Firefox, IE9) oder **Ghostery** (Firefox, IE9, Chrome, Opera, Safari)
- **Panopticlick**: Zeigt online, wie gut individualisierbar Sie im Internet sind
- **FPDetective**: kann Fingerprinting entdecken
- **Lightbeam**: visualisiert das Beziehungsnetz, auf das sich einlässt, wer werbefinanzierte Websites aufruft
- für bessere Sicherheit: **Onion Browser** (iOS) und **Tor Browser Bundle** (Windows, Mac, Linux)

In öffentlichen Netzen keine heiklen Transaktionen starten (Banking, Bestellportale)! Nicht auf Hyperlinks in zugesandten E-Mails klicken, sondern URL eintippen.

Messenger/SMS/MMS

WhatsApp (OS, Android)**:** Lädt das ganze Adressverzeichnis auf externe Server. Beteuerte immer, die Daten der Nutzer weder zu sammeln noch kommerziell zu verwerten. Nach dem Kauf durch Facebook (für 19 Mia Dollar) ist nicht klar, was mit den Informationen geschieht.

iMessage (iOS)**:** verschlüsselte Übermittlung, kann von Apple aber entschlüsselt werden.

iO: von Swisscom, für iOS und Android. Verschlüsselte Verbindung, kein Upload des Adressverzeichnisses. SMS und Telefonate.

Threema (Server in der Schweiz): iOS und Android, End-zu-End-Verschlüsselung des Inhalts. Anonyme ID der Benutzer.

Wickr: iOS und Android, End-zu-End-Verschlüsselung, keinerlei Speicherung von Daten auf den Servern, auch Metadaten werden gelöscht. Server in den USA.

TorChat (Windows, Linux) (Tor-Netzwerk)

Hoccer XO: iOS und Android: End-zu-End-Verschlüsselung (iOS, Android, Blackberry)

Telegram Messenger: End-zu-End-Verschlüsselung möglich, selbstvernichtende Nachrichten möglich (iOS und Android, Mac, Windows, Internet-Browser)

in Vorbereitung: **TIMB**, basierend auf Tor-Netzwerk

E-Mail

Privasphere, Verschlüsselung der *Übertragung*, kein Konnex zwischen Absender und Empfänger sichtbar. Läuft auf Schweizer Servern. Täglich 3 E-Mails gratis.

Incamail: Sichere, nachweisbare, verschlüsselte Zustellung.

Inhalt verschlüsseln mit **Truecrypt** oder **AxCrypt** (Windows)**;** symmetrische Schlüssel

E-Mail-Adresse: ohne Verwendung des richtigen Namens.

Mehrere E-Mail-Adressen für selten verwendete Dienste verwenden; Wegwerf-Adressen für Anmeldung auf selten besuchten Websites (z.B. www.byom.de, www.instant-mail.de).

Keine Beilagen von E-Mails unbekannter Herkunft öffnen; keine Hyperlinks anklicken, sondern den angegebenen URL eintippen.

mailbox.org in der BRD: mit https-Verbindung, PFS und verschlüsseltem Postfach

BitMessage-Protokoll: Asymmetrische Verschlüsselung, Broadcast-Prinzip (Adressat nicht erkennbar, Versand an eine ganze Gruppe von Personen, wobei nur der gewünschte Empfänger den Inhalt lesen kann). Im Moment noch ein Projekt bzw. Proof of Concept. Die in Entwicklung befindliche Software ist nicht fehlerfrei und liegt bei der Benutzerfreundlichkeit hinter dem üblichen E-Mail zurück.

Verschlüsselung

Standard: **Perfect Forward Secrecy**, mit Diffie-Hellman-Schlüsselaustausch: Flüchtige, vergängliche Schlüssel. Nur bei Google, gmx.de und web.de eingesetzt.

Software: **Truecrypt**, **Pretty Good Privacy**

VPN verwenden (Virtual Private Network)

DARPA-Projekt: Homomorphic Encryption

Firewall

Two-Way Firewalls einsetzen (Firewall in beiden Richtungen). Während der normale Router darauf achtet, dass keine ungewünschten Zugriffe von aussen erfolgen, kontrolliert ein Two-Way Firewall neben dem eingehenden Datenverkehr auch den vom PC/Mac ausgehenden Datenverkehr.

- Mac: **Little Snitch** Netzwerkwächter
- PC: **NetLimiter Window**, **Jetico Personal Firewall**, **Windows 8 Firewall Control** (Sphinx Software); **Outpost Firewall Pro**, **ZoneAlarm**

Telefonieren

Generell: Handy nie (nie!) aus der Hand geben!

Bei vertraulichen Gesprächen: Handy wegschliessen.

Handy-Apps für verschlüsselte Kommunikation:

- **RedPhone** (Android)
- **Cellcrypt** (iOS, Android, Blackberry, Symbian).
- **Chiffry** (im Moment nur für Android und deutsche Nummern, inkl. Telefon, SMS, MMS, Gruppenchat, Sprachnachrichten, Videos versenden). Schlüsseltausch auf Basis der modernen Elliptische-Kurven-Kryptografie (512-Bit ECDH) sowie eine Benutzeridentifizierung mittels spezieller Zertifikate. Der Fälschungsschutz aller mit Chiffry versendeter Nachrichten und Inhalte wird zusätzlich durch sichere Signaturen gemäss dem 512-Bit ECDSA-Standard gewährleistet.

Hardware-Lösungen:

- Verwendung einer speziellen Micro-SD-Card (z.B. **Crypto Mobile HC-9100**, für Nokia-Handys)
- Abhörsicheres Telefon: **Simko 3**; basierend auf Galaxy S3, mit eigenem Betriebssystem. Nachteile: anscheinend geringe Akkulaufzeit und Fehlen wichtiger Funktionen wie WLAN, Kamera und Bluetooth.
- Blackberry mit **SecuSuite**

Kommerzielle Anbieter verschlüsselter Kommunikation:

- In der Schweiz: www.e-fon.ch, www.infoguard.ch
- www.globaliptel.com
- www.securstar.com
- www.voiponeclick.com
- www.coverme.ws
- www.crypto.ch (professionelle Chiffriergeräte)

iOS-Handy

Zugangscode festlegen, mind. 5-stellig[4], mit automatischer Sperre

Kein Jailbreak; nur Apps aus dem offiziellen Store installieren

Passwort-Apps

- **GetStrip** (Windows, Mac, iOS, Android; mit lokalem Backup via WLAN)
- **1Password** (Windows, Mac, iOS, Android)
- **MiniKeePass** (nur iOS)
- **Private Pal** (nur iOS)
- **iPIN** - Secure PIN & Passwort Safe (iOS, Android, Mac, Windows)
- **OneKey Pro** (iOS)
- **pwSafe**

Aus Sicherheitsgründen sind Apps vorzuziehen, die nur lokal synchronisieren (via WLAN oder Kabel), nicht via Cloud.

[4] Einstellungen/Code

Sicherheits-Massnahmen:

- **Find my iPhone** installieren und aktivieren, oder **Prey** (grösserer Funktionsumfang)
- "Apps löschen" deaktivieren[5]
- Internet-Zugang nur für Programme zulassen, die dies unbedingt brauchen[6]
- Ortungsfunktion nur dort zulassen, wo es unbedingt nötig ist[7]
- Mikrofon-Funktion nur dort zulassen, wo es unbedingt nötig ist[8]
- Zugriff auf die Kontakte und Kalender nur jenen Apps erlauben, die dies unbedingt benötigen[9]
- Ad-Tracking ausschalten[10]
- Bluetooth abstellen wenn nicht gebraucht
- iCloud-Zugriff der Apps restriktiv definieren.[11]
- Tethering (Persönlicher Hotspot) abstellen wenn nicht gebraucht
- Automatische Rückmeldungen an Apple unterbinden[12]

Android-Handy

Software grundsätzlich nur aus dem offiziellen Store beziehen; Ausnahmen gut absichern.

Zugangscode festlegen.

Sicherheits-Apps:

- **EDS Lite** für Verschlüsselung von Dateien
- Passwort-Tresor (Achtung: Übergabe via Clipboard nicht benützen, da alle Apps auf das Clipboard zugreifen können):
  - **SecureSafe**
  - **KeePassDroid**
  - **Keepass2Android**
  - **aWallet**
- Mit **App Lock** schützen Sie Ihre installierten Anwendungen mit einem Passwort oder Muster.
- Wiederfinden/Sperren des verlorenen Handys:
  - **Lookout**
  - **Avira Free Android Security**
  - **AndroidLost**
- gegen Werbe-Einblendungen: **Lookout Ad Network Detector**
- Tethering (Persönlicher Hotspot) abstellen wenn nicht gebraucht
- Im Weiteren: siehe oben unter "iOS-Handy/Sicherheitsmassnahmen"

[5] Einstellungen/Allgemein/Einschränkungen
[6] Einstellungen/Mobiles Netz
[7] Einstellungen/Allgemein/Hintergrundaktualisierungen bzw. Einstellungen/Allgemein/Einschränkungen/Ortungsdienste
[8] Einstellungen/Datenschutz
[9] Einstellungen/Allgemein/Einschränkungen/Kontakte
[10] Einstellungen/Datenschutz/Werbung bzw. …/Kalender
[11] Einstellungen/iCloud
[12] Einstellungen/Allgemein/Info/Diagnose und Nutzung

Social Media

Via Computer-Spiel der Uni Regensburg ("Friend Inspector") können Sie aufklären, wie es um Ihre individuelle Privatsphäre steht bei Facebook.

- Verwenden Sie einen Alias-Namen
- Stellen Sie die Datenschutz-Einstellungen auf maximal
- Verwenden Sie in Ihrem Profil ein Symbolbild statt eines Portraits
- Üben Sie Zurückhaltung bei der Bekanntgabe von Lebensdaten und Tätigkeiten
- "Posten" Sie keine heiklen Informationen

Twitter: Apple hat für 200 Mio Dollar alle seit 2006 weltweit abgesetzten Tweets aufgekauft – inkl. Bilder, Videos und Hashtags – und wertet sie aus.

Bei Anmeldung auf selten besuchten Websites Alias-Namen und falsches Geburtsdatum, Anschrift, Telefon-Nummer verwenden; Wegwerf-E-Mail-Adressen benützen.

Kreditkarten, Bankkarten

Geben Sie sie nie (nie!) aus der Hand

Zahlungen im Internet nur via https-Sites.

Gewisse Kreditkartenherausgeber stellen Ihnen auf Wunsch nach jeder Belastung eine SMS zu.

Zahlungen via Kreditkarte können von Nachrichtendiensten überwacht werden. Bei Zahlungen via Bankkarte (Maestro) ist dies nicht ohne Weiteres möglich.

Information

The Intercept: Publizistische Website, hinter der Glenn Greenwald und andere Reporter stehen, die die Snowden-Dokumente als erste publiziert haben. Zu den zentralen Themen von The Intercept gehören Korruption, Machtmissbrauch und die Verletzung von Bürgerrechten.

The Guardian: Englische Zeitung, die als erste und seither regelmässig und fundiert über die Überwachungspraktiken der Nachrichtendienste berichtet.

Frankfurter Allgemeine mit spezieller Rubrik zu diesem Thema.