dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Datenschutzfreundliche Software

In diesem Merkblatt wird eine Auswahl Windows-, MacOS- und Linux-Software zu folgenden Themen vorgestellt:

1 Anonymes Suchen
2 Anonymes Surfen
3 Sicheres Surfen
4 Verhindern von Webtracking
5 Sicheres Löschen
6 Löschen temporärer Daten
7 Sicheres Arbeiten (IT-Arbeitsumgebung)
8 Datenschutzfreundliche Nutzung von Karten
9 Datenschutzfreundliche Konfiguration
10 Sicheres Speichern der Passwörter
11 Schutz vor Trojanern und Spyware
12 Sicheres Kommunizieren
13 Aktualisierung des Betriebssystems und Applikationen
14 Verschlüsselung der Daten

1 Anonymes Suchen

Anonyme Suchdienste ermöglichen Suchabfragen im Internet, ohne dass der Suchmaschinenbetreiber mit den gespeicherten Daten ein Persönlichkeitsprofil erstellen kann.

- DuckDuckGo
- etools.ch
- MetaGer
- Startpage
- YaCy (Unabhängige Peer-to-Peer-Suchmaschine. Für die Nutzung muss eine Java-Software installiert werden)

2 Anonymes Surfen

Wer im Internet surft, hinterlässt seine IP-Adresse und andere Spuren. Mit der entsprechenden Software können diese Spuren teilweise verhindert oder unkenntlich gemacht werden.

- Hide My Ass Web Proxy (Keine Installation von Software erforderlich)
- JAP
- Tor Browser

3 Sicheres Surfen

Beim Surfen besteht ein hohes Risiko einer Vireninfektion. Mit einer geeigneten Browsererweiterung lässt sich dieses Risiko stark reduzieren. Standardmässig blockieren diese Erweiterungen Javascript und andere dynamische Inhalte (White-List-Ansatz).

- NoScript (Firefox)
- NotScripts (Opera)
- ScriptSafe (Chrome)

4 Verhindern von Webtracking

Webtracking wird von Werbenetzwerken eingesetzt, um das Surfverhalten von Internetnutzerinnen und Internetnutzern zu erfassen. Die damit erhobenen Daten ermöglichen es, Rückschlüsse auf die Interessen, Vorlieben oder Gewohnheiten der Benutzenden zu ziehen. Mit einer geeigneten Browsererweiterung lässt sich dies zu einem grossen Teil verhindern.

- Ghostery (Firefox, IE, Safari, Chrome und Opera)
  Blockieren der Trackingdienste beim Surfen
- Self-Destructing Cookies (Firefox)
  Automatisches Löschen von Cookies

- Weiterführende Informationen in der Checkliste Webtracking verhindern

5 Sicheres Löschen

Beim Löschen von Dateien wird oft nur die Referenz auf eine Datei entfernt und der eigentliche Inhalt bleibt bis zum nächsten Überschreiben erhalten. Mit entsprechender Software lassen sich die Dateien wiederherstellen. Um dies zu verhindern, überschreibt die folgende Software die Dateien mehrmals.

- Eraser (Windows)

6 Löschen temporärer Daten

Beim Arbeiten am Computer fallen temporäre Dateien oder Metadaten an, die explizit gelöscht werden müssen. Mit der folgenden Software können diese Dateien gesucht und gelöscht werden.

- CCleaner (Windows und MacOS)
- ClearProg (Windows)
- GClean (Windows, kostenpflichtig)
- ImageOptim (MacOS)
- JPEG & PNG Stripper (Windows)
- PrivaZer (Windows)

7 Sicheres Arbeiten (IT-Arbeitsumgebung)

Für sensitive Aufgaben (beispielsweise E-Banking) existieren spezielle, nicht beschreibbare (read-only) Betriebssysteme, die ab CD / DVD oder USB-Stick (falls vorhanden mit Schreibschutz) gestartet werden. Somit können die Arbeiten innerhalb einer geschützten Umgebung ausgeführt werden.

- InvestigateIX
- Tails

8 Datenschutzfreundliche Nutzung von Karten

Der bekannteste Kartenanbieter Google Maps verknüpft die Nutzungsdaten mit weiteren Informationen und bildet damit ein umfassendes Persönlichkeitsprofil. Die folgenden Kartendienste sind datenschutzfreundliche Alternativen.

- GIS-Browser – Kanton Zürich (nur Kanton Zürich)
- Kartenviewer – Schweizerische Eidgenossenschaft
- OpenStreetMap

9 Datenschutzfreundliche Konfiguration

Systeme datenschutzfreundlich zu konfigurieren, ist teilweise sehr aufwendig. Softwarelösungen bieten Hilfestellung an.

- Facebook Privacy Watcher (Firefox und Chrome)
- xpy (Windows)

10 Sicheres Speichern der Passwörter

Passwörter sollen nicht aufgeschrieben und für jeden Dienst soll ein eigenes gewählt werden. Diverse Softwarelösungen bieten Unterstützung an, um die Passwörter sicher abzuspeichern und automatisiert einzugeben. Der Datenschutzbeauftragte empfiehlt, Passwörter für sensitive Bereiche nicht mit diesen Tools zu verwalten.

- KeePass2 (Windows, MacOS und Linux)
- LastPass (Windows, MacOS und Linux)

- Weiterführende Informationen im Merkblatt Passwortmanager

11 Schutz vor Trojanern und Spyware

Die Sicherheit beim Surfen im Internet kann mit geeigneten Schutzprogrammen beispielsweise mit einem Virenschutz oder einer Personal Firewall erhöht werden.

11.1 Virenschutz

- Avast (Windows)
- Avira (Windows und MacOS)
- Microsoft Security Essentials (Windows)

11.2 Personal Firewall

- Comodo Internet Security (Windows)
- ZoneAlarm (Windows)

12 Sicheres Kommunizieren

Die unverschlüsselte Kommunikation, beispielweise per E-Mail, kann einfach mitgelesen werden. Für die verschlüsselte und sichere Kommunikation existieren diverse Softwarelösungen.

- Cryptocat (Windows, MacOS und Linux)
  Chat
- Enigmail (Mozilla Thunderbird; Windows, MacOS und Linux)
  E-Mailverschlüsselung mit PGP
- Gpg4win (Windows)
  E-Mailverschlüsselung mit PGP (GnuPGP)
- GPGTools (MacOS)
  E-Mailverschlüsselung mit PGP (GnuPGP)
- Jitsi (Windows, MacOS und Linux)
  Nachrichten und Telefonie
- Pidgin (Windows und Linux; MacOS: adium)
  Chat

13 Aktualisierung des Betriebssystems und Applikationen

Regelmässiges Aktualisieren des Betriebssystems des Computers und der darauf installierten Anwendungen hilft, einem möglichen Malwarebefall vorzubeugen. Das folgende Programm prüft, ob die installierte Software auf dem Computer aktuell ist.

- Flexera Personal Software Inspector (Windows)

14 Verschlüsselung der Daten

Unverschlüsselt abgespeicherte Daten sind für jede Person mit Zugriff auf die Festplatte lesbar. Dies ist insbesondere bei Diebstahl, Verkauf oder Verlust des Geräts problematisch. Deshalb sollten entweder die komplette Festplatte oder mindestens die sensitiven Dateien verschlüsselt werden. Die folgenden Softwarelösungen sind auch hilfreich, um zum Beispiel Dateien sicher in der Cloud zu speichern.

- 7-Zip (Windows)
  Erstellen verschlüsselter Zip-Archive (AES)
- AxCrypt (Windows)
- Bitlocker (Windows)
  Verschlüsselung für USB-Sticks, Festplatten und Cloud
- Boxcrypter (Windows, MacOS und Linux)
  Verschlüsselung für Online-Speicherdienste
- Cryptomator (Windows, MacOS, Linux, Android und iOS)
  Verschlüsselung für Online-Speicherdienste
- HTTPS Everywhere (Firefox und Chrome)
  Automatischer Wechsel auf https-Seiten
- VeraCrypt (Windows, MacOS und Linux)
  Verschlüsselung für USB-Sticks, Festplatten und Cloud
- WinRar (Windows, MacOS und Linux, kostenpflichtig)
- WinZip (Windows und MacOS, kostenpflichtig)
- Wise Folder Hider (Windows)
  Verstecken von Dateien

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
Fax 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch