DIGITAL SECRETS

SIN Studio im Netz

Festplatten-Verschlüsselung:

BitLocker: Ein Microsoft-Programm zur Festplattenverschlüsselung. Es schützt mit Hilfe von TPM (Trusted Platform Module) das Windows-Betriebssystem und alle Benutzerdateien. BitLocker ist proprietär und nur für Windows verfügbar. http://windows.microsoft.com/de-de/windows/protect-files-bitlocker-drive-encryption

VeraCrypt: Ermöglicht die Verschlüsselung von Ordnern, Festplatten, Wechseldatenträgern oder auch dem gesamten System. VeraCrypt ist kostenlos und als Open-Source verfügbar. https://veracrypt.codeplex.com/

TrueCrypt: Der „Urvater" der Verschlüsselungstools für diverse Plattformen. Obwohl TrueCrypt nicht mehr weiterentwickelt wird, ist es immer noch der De-facto-Standard und enthält keine Sicherheitslücken. http://www.heise.de/download/truecrypt.html

E-Mail-Verschlüsselung:

GnuPG: Open-Source-Programm zur Verschlüsselung von E-Mails, das auf dem standardisierten Datenformat Open PGP basiert. Die verschlüsselten Daten können mit einem Schlüssel geöffnet werden, der vom Sender an den Empfänger übergeben wird. Zudem sind die User über eine digitale Signatur authentifiziert. https://www.gnupg.org

GPG4Win: GnuPG-Implementierung für Windows, kostenlos und mit öffentlichem Quellcode. Das Programm unterstützt bei der Einrichtung eines privaten Schlüssels und bietet Tools zum Ver- und Entschlüsseln von Daten an. https://www.gpg4win.de/

Enigmail: Ein Plugin für Mozillas E-Mail-Client Thunderbird. Mit Enigmail lassen sich verschlüsselte und/oder signierte E-Mails versenden. Der Schlüssel lässt sich in Enigmail direkt oder über Drittsoftware wie GPG4Win erzeugen. https://www.enigmail.net

K-9 Mail: Kostenlose und quelloffene App für Android, die die Einrichtung mehrerer E-Mail-Konten ermöglicht. Eine Mail-Verschlüsselung ist mithilfe weiterer Software wie OpenKeychain möglich. https://play.google.com/store/apps/details?id=com.fsck.k9

ProtonMail: Ein quelloffener und kostenfreier E-Mail-Dienst der Forschungseinrichtung CERN, der einen verschlüsselten E-Mail-Verkehr ermöglicht. ProtonMail ist als App für Android und iOS sowie als Web-Anwendung benutzbar. https://protonmail.com/

Cloudspeicher-Verschlüsselung:

BoxCryptor: Eine Verschlüsselungssoftware für Dateien, die in Cloud-Speicherdiensten wie Dropbox, Google Drive uvm. abgelegt werden. Die proprietärer Software ist für Privatanwender kostenlos. https://www.boxcryptor.com/de/boxcryptor

Whisply: Neues Online-Tool von BoxCryptor, das ebenfalls Dateien vor dem Cloud-Upload verschlüsselt. Das Tool ist mit Dropbox, Google Drive und Microsoft One Drive kompatibel und benötigt keine zusätzliche Anmeldung. https://whisp.ly/de

Browser-Erweiterungen:

HTTPS Everywhere wandelt die unverschlüsselte Datenübertragung auf Webseiten in eine verschlüsselte Übertragung um. Die freie Software ist kostenfrei für Mozilla Firefox und Google Chrome erhältlich. https://www.eff.org/HTTPS-everywhere

noScript blockiert JavaScripts, Java-Applets, Flash- und Silverlight-Animationen. Das Tool steht unter freier GNU-Lizenz und ist kostenfrei, jedoch nur für Mozilla Firefox erhältlich. https://noscript.net/ (ähnliches Tool für Chrome: ScriptSafe)

uBlock Origin ist ein quelloffenes, kostenfreies Browser-Plug-In, das Inhalte wie Werbung und Tracking-Anfragen blockiert. https://github.com/gorhill/uBlock

Ghostery ist ein proprietäres Add-on, das Cookies verschiedener Kategorien blockiert. Ghostery gibt es kostenfrei für verschiedene Web-Browser sowie als Browser-App für Android und iOS. https://www.ghostery.com/

Smartphone-Apps und -Einstellungen:

Smartphone-Verschlüsselung: Android-Phones lassen sich über die Systemeinstellungen verschlüsseln, eine Anleitung dazu findet sich z.B. unter https://www.androidpit.de/ist-android-verschluesselung-sinnvoll. Auch für iOS-Geräte ist eine Hardware-Verschlüsselung möglich, die hier erklärt wird: https://support.apple.com/de-de/HT202064

Messenger: Datenschutzkonforme Messenger mit Verschlüsselung der Nachrichten sind z.B. die freien Apps **Signal** (https://whispersystems.org/) und **Wire** (https://wire.com/) sowie die proprietären Apps **Threema** (https://threema.ch/) und **Telegram** (https://telegram.org/). Überblick siehe https://www.eff.org/secure-messaging-scorecard

App-Berechtigungen überprüfen: Um einen Überblick darüber zu erhalten, welche Apps sich welche Zugriffsrechte einräumen, ist z.B. die kostenlose App „My Permissions“ hilfreich. Sie ist für Android und iOS sowie als Browser-Erweiterung erhältlich unter https://mypermissions.de/. Ähnlich funktioniert die kostenlose App Clueful, die nur für Android angeboten wird, http://www.bitdefender.de/solutions/clueful-android.html.

Datenschutz-Einstellungen: Die Seite mobilsicher.de liefert umfangreiche Checklisten zur Sicherung mobiler Geräte, unter https://mobilsicher.de/2015/08/28/basissicherung/ für Android und iOS, www.mobilsicher.de/2015/09/07/basissicherung-fuer-ios-geraete.

Smartphone-Sicherheit: Zahlreiche Apps werben damit, die Sicherheit mobiler Geräte zu erhöhen. Eine unabhängige Quelle mit aktuellen Informationen zur Online-Sicherheit ist das Bundesamt für Sicherheit in der Informationstechnik, das auf der Seite „BSI für Bürger“ informiert: https://www.bsi-fuer-buerger.de/

Weitere Links:

- **Bundesbeauftragte für Datenschutz und Informationsfreiheit:** www.bfdi.bund.de
- **Informationsangebot deutscher Datenschutzinstanzen:** www.datenschutz.de
- **Blog von IT- und Datenschutz-Spezialisten:** www.datenschutzbeauftragter-info.de
- **TOR-Projekt (Programme und Apps für Online-Anonymität):** www.torproject.org

Zusammenstellung von SIN – Studio im Netz, www.studioimnetz.de, im September 2016