Digitale Selbstverteidigung

Datenskandale, Datenkommerzialisierung und digitale Überwachung: Nutzerinnen und Nutzer müssen ihren Datenschutz weitgehend selbst in die Hand nehmen. In erster Linie gelingt dies mit vorsichtigem Online-Verhalten, sicheren Passwörtern sowie regelmässigen Updates und Backups. Folgende Anregungen können Privatpersonen helfen, Datensammlern die Arbeit schwerer zu machen. Vor Überwachung durch autoritäre Staaten und Geheimdienste sowie vor ausgeklügeltem Hacking können sie aber nicht ausreichend schützen. Wenn ein Angebot «gratis» ist, muss man annehmen, dass es sich durch den Verkauf von Daten finanziert. Wichtig ist, sich Gedanken darüber zu machen, vor welchen Gefahren man sich schützen möchte – und sich im Zweifelsfall professionelle Unterstützung zu suchen.

Passwörter

Ein gutes Passwort besteht aus einer grossen und zufälligen Anzahl von Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. Für jede Anwendung sollte ein individuelles Passwort verwendet werden. Dafür kann eine Passwort-Manager-Software hilfreich sein.

Smartphone-Sicherheit

Es empfiehlt sich, einen Code und die automatische Gerätesperre zu aktivieren. Um die Sicherheit zu erhöhen, müssen regelmässig Software-Updates durchgeführt werden. Ausserdem sollte man Apps nur aus vertrauenswürdigen Quellen installieren und ungenutzte Apps deinstallieren. Neben mehr Speicherplatz verringert sich dadurch das Risiko, dass im Hintergrund unbemerkt Daten gesammelt werden. Regelmässige Backups helfen davor, Daten zu verlieren.

Öffentliche Netzwerke können erhebliche Sicherheitslecks aufweisen und sollten daher keinesfalls für sensible Transaktionen wie Online-Banking genutzt würden. Gute VPN-Clients schaffen in öffentlichen Netzwerken Abhilfe, verlangsamen aber das Surfen. Um ungewollte Datenübermittlung zu vermeiden und zudem Akku zu sparen, sollten drahtlose Schnittstellen wie Ortungsdienste, WLAN und Bluetooth deaktiviert werden, wenn sie nicht genutzt werden. Es ist ratsam, den Zugriff einzelner Apps auf Ortungsdienste, Kontakte, Mikrofon, Kamera, Bewegungs- und Fitnessdaten regelmässig zu überprüfen und zu beschränken. Auch das Werbe-Tracking kann in den Smartphone-Einstellungen eingeschränkt werden. Wer das Smartphone regelmässig als Hotspot nutzt, kann den Namen des Geräts ändern, damit der eigene Name nicht öffentlich einsehbar ist.

Bei Verlust sollte man das Gerät über die Suchfunktion lokalisieren, die SIM-Karte sperren lassen und Passwörter wechseln. Bevor man sein Gerät verkauft oder entsorgt, sollten noch vorhandene Daten sauber gelöscht werden.

Sichere Nachrichten und E-Mails

Die technische Herausforderung, Nachrichten und E-Mails zu verschlüsseln, ist kleiner, als die eigenen Kontakte davon zu überzeugen, diese Dienste auch tatsächlich zu nutzen. WhatsApp nutzt zwar inzwischen Ende-zu-Ende-Verschlüsselung, gehört allerdings der Firma Facebook, die zwar die verschlüsselten Nachrichten nicht mitlesen, aber Metadaten speichern kann (beispielsweise: wer wann mit wem Kontakt hat).

Threema ist eine Schweizer WhatsApp-Alternative mit konsequenter Ende-zu-Ende-Verschlüsselung. Der Messenger Signal wird von einer gemeinnützigen Stiftung entwickelt. Er ist für seine Datensparsamkeit und Ende-zu-Ende-Verschlüsselung bekannt. Zudem ist Signals Software Open Source, was auch aus Sicherheitssicht begrüssenswert ist. Apples iMessage erhält von Expertinnen und Experten im Bereich Cybersicherheit ebenfalls regelmässig gute Noten.

Die eigene E-Mail-Adresse sollte man sparsam bekanntgeben. Es kann sich zudem lohnen, verschiedene Adressen für verschiedene Zwecke einzurichten. Ob die eigene Adresse schon mal über ein Datenleck veröffentlicht wurde, kann man unter haveibeenpwned.com überprüfen. Keinesfalls sollte man Angaben über Benutzeridentifikationen, Passwörter, Konto- und Kreditkartennummern oder sonstige Zugangsdaten per E-Mail weitergeben. Bei E-Mails mit unbekannten Absendern empfiehlt es sich, weder auf Links zu klicken noch Dateianhänge zu öffnen. Unter send.firefox.com können Dateien einfach Ende-zu-Ende-verschlüsselt und kostenlos verschickt werden. ProtonMail ist ein kostenfreier E-Mail-Dienst, der die Nachrichten verschlüsselt. Profis verschlüsseln ihre E-Mails mit PGP oder GPG. Diese Programme ermöglichen ein sicheres, jedoch vergleichsweise anspruchsvolles Public-Key-Verschlüsselungsverfahren. Dennoch bleiben Metadaten trotz Verschlüsselung der Inhalte zugänglich. Zudem kann Schadsoftware Texte nach der Entschlüsselung abfangen oder Passwörter mitloggen.

Surfen und Suche

Firefox ist unter Datenschutzbewussten der Browser-Klassiker. Er wird von der gemeinnützigen Mozilla Foundation betrieben. Ausserdem können zahlreiche Datenschutz- und Privatsphäre-Einstellungen vorgenommen werden wie das systematische Löschen von Cookies und Chronik. Der Browser-Zusatz HTTPS Everywhere erhöht die Online-Sicherheit. Brave, Red Browser und Tor sind weitere Browser, die sich dem Datenschutz verschrieben haben. Ghostery und Disconnect weisen beim Surfen auf versteckte Dienste hin, die im Hintergrund private Daten übermitteln, und blockieren diese auf Wunsch.

Verschiedene Internet-Firmen stehen in Bezug auf Datenschutz in der Kritik. Dazu gehören beispielsweise die Firma Alphabet (zu der auch Google mit Websuche, Android, YouTube, Chrome-Browser und Gmail gehören), die Firma Facebook (zu der auch Instagram und WhatsApp gehören) und Amazon. Wer dennoch nicht auf die nützlichen Dienste z.B. von Google verzichten möchte, kann unter myactivity.google.com nachsehen, was Google über einen speichert. Dort kann man teilweise einschränken, was getrackt werden darf: Web- und App-Aktivitäten, das YouTube-Verhalten, das Bewegungsprofil über den Standortverlauf, Einstellungen zu personalisierter Werbung. Die Suchmaschinen DuckDuckGo und Startpage.com sind datenschutzfreundliche Alternativen. Nach eigenen Angaben stellen sie keine Nutzerprofile her und sammeln keine Daten. Statt Google oder Apple Maps bieten auch OpenStreetMap, Schweiz Mobil und map.geo.admin.ch Orientierung.

Sprachassistenten und Smart-Lautsprecher wie Amazons Alexa, Apples Siri und der Google Assistant sind nützlich, um per Sprachbefehl online den Wetterbericht abzurufen, Bestellungen aufzugeben oder eine Musik-Playlist zu starten. Verschiedene Gutachten warnen jedoch vor unerwünschter Datensammlung und Aufzeichnung intimer Momente zu Hause, weil diese Angebote standardmässig das Mikrofon aktiviert haben und die Datenauswertung intransparent sei.

Social Media

Dienste wie Facebook, Twitter, Instagram und Snapchat speichern neben den Inhalten, die wir selbst teilen, zusätzlich Metadaten wie Standort, Kontakte und Interessensgebiete, um personalisierte Werbung einblenden zu können. Das ist Teil ihres Geschäftsmodells. Dennoch bieten diese Dienste oft die Möglichkeit, Datenschutz- und Privatsphäre-Einstellungen zu optimieren und die Sichtbarkeit von Beiträgen einzuschränken.

Cyberkriminalität und Erpressung

Das Bundesamt für Polizei fedpol warnt unter fedpol.admin.ch vor verschiedenen Formen von Cyberkriminalität wie Phishing, Hacking und Pädokriminalität. Wenn Unbekannte per E-Mail behaupten, Zugang zu Computer und Webcam zu haben, und damit drohen, kompromittierendes Bild- oder Videomaterial zu veröffentlichen, sollte man weder antworten noch Lösegeld bezahlen. Auch deswegen kleben viele ihre Webcams ab. Zur Information und Hilfe bei Erpressungsfällen gibt es unter stop-sextortion.ch eine Anlaufstelle, die verschiedene Schweizer Polizeibehörden sowie die Schweizerische Kriminalprävention betreiben.

Aktuelles zu Sicherheit und Datenschutz

Die offizielle Schweizer Melde- und Analysestelle Informationssicherung MELANI bietet unter melani.admin.ch aktuelle Informationen zur Bedrohungslage für private Computer- und Internetnutzerinnen und -nutzer sowie für Unternehmen: beispielsweise über aktuelle Angriffe durch Phishing-E-Mails, Verschlüsselungstrojaner oder gefälschte SMS. Wer selbst von Viren und Würmern betroffen ist, kann dort Meldeformulare ausfüllen.

Die Datenschutz.ch-App des Datenschutzbeauftragten des Kantons Zürich bietet Informationen über die wichtigsten Rechte zum Schutz der Daten und der Privatsphäre, Tools, um die eigene Datensicherheit zu verbessern, und konkrete Hilfestellungen für spezifische Fachbereiche, aber auch für Privatpersonen.

Quellen und Anlaufstellen: Digitale Gesellschaft digitale-gesellschaft.ch, Chaos Computer Club Schweiz ccc-ch.ch, Netzpolitik netzpolitik.org, Electronic Frontier Foundation eff.org, Tactical Tech tacticaltech.org, Privacy Tools privacytools.io, Melde- und Analysestelle Informationssicherung Melani melani.admin.ch, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter edoeb.admin.ch, Datenschutzbeauftragter Kanton Zürich datenschutz.ch. Digitale Selbstverteidigung für Profis (in Englisch): «Surveillance Self-Defense» der Electronic Frontier Foundation ssd.eff.org und «Data Detox Kit» der Mozilla Foundation und Tactical Tech datadetoxkit.org.

Redaktion: Dr. Sarah Genner im Rahmen der Ausstellung im Stadthaus «Privatsphäre – geschützt, geteilt, verkauft» (19.9.19–29.2.20) von Stadt Zürich Kultur in Zusammenarbeit mit dem Collegium Helveticum.