Ein Text von: **CARL-JOSEF KUTZBACH**

Notiert am: 10.1.2019 poschd@cajo-kutzbach.de

Bequem oder sicher

Weshalb Daten selten sicher sind

Als am 4. Januar klar wurde, dass die Daten von Hunderten von Politikern, Prominenten und Journalisten veröffentlicht worden waren, war der Spott groß, aber das ist nicht ganz gerecht, denn moderne Programme und Geräte sind darauf ausgelegt den Herstellern viele Informationen über das Verhalten der Benutzer zu übermitteln. Man fühlt sich an den Satz erinnert: „Thats not a bug, that's a feature!“ mit dem ein Hersteller den Kunden weiß machen wollte, dass das, was aus ihrer Sicht nicht funktionierte (ein Bug, ein „Käfer“), in Wirklichkeit eine wohl durchdachte Anwendungsmöglichkeit sei.

Wenn aber viele Programme und Geräte auf das Übermitteln von Daten ausgelegt sind, dann braucht man sich nicht wundern, wenn es auch dann passiert, wenn man das gar nicht beabsichtigt. Wenn man sich das Internet als ein großes Fischernetz vorstellt, dann kann es immer wieder vorkommen, dass eine oder mehrere Maschen dieses Netzes ein Loch haben. Deshalb kontrollieren Fischer ihre Netze immer wieder und flicken solche Löcher, damit ihnen die Fische nicht aus dem Netz entkommen. Das Internet dagegen hat keinen Fischer, der sich um den Zustand des Netzes kümmert und Maschen flickt, wenn se defekt sind, weil es eine dezentrale Struktur ist, auch, wenn die großen Telekommunikationsverbindungen und ihre Leitungen sozusagen das Rückenmark des Internets sind.

Daher dürfte der verstorbene IT-Fachmann Paul Liller recht haben, der meinte: „Wer ins Netz geht, wird früher oder später gehackt (angegriffen).“ Das kann ein verhältnismäßig harmloser Angriff sein, von jemand der vor allem wissen will, ob er weiß, wie es geht, aber es kann auch dazu dienen Betroffene unter Druck zu setzen, indem man Daten stiehlt, oder den Rechner blockiert. Die Bemühungen Wähler beim Brexit, bei der Wahl des US-Präsidenten und beim Niedergang von Demokratien in Afrika durch Informationen, die zumindest teilweise falsch waren, im Sinne der Urheber zu beeinflussen liefen alle über Facebook und die inzwischen umbenannte Firma Cambridge Analytica, wie Forscher der Max-Planck Gesellschaft fanden. Facebook gibt oder gab die Daten seiner Nutzer an über 150 Firmen weiter.

Dieses Beispiel zeigt, dass längst Firmen auf die Politik Einfluss nehmen, ohne, dass sie dazu von den Wählern legitimiert worden wären. Dasselbe geschieht teilweise bei Suchmaschinen, deren Berechnungsverfahren (Algorithmen) meist geheim sind. Hinzu kommt, dass die Anbieter so tun, als ob die Suche kostenlos wäre, weil sie sich über Werbung finanzierten. Dass sie auch an den Daten verdienen, die sie von den Nutzern (oft ohne deren bewusste Zustimmung) bekommen, lässt man ebenfalls lieber im Dunkeln. Nur wer sich die Mühe macht die Geschäftsbedingungen oder die Datenschutz-Erklärung zu lesen, erfährt, welche Daten erhoben werden, ob sie weiter gegeben werden, oder was damit passiert. Aber wer macht das? Ein Rechtsanwalt meinte mal: „Ich habe nur die Wahl zuzustimmen, oder auf die Nutzung des Dienstes zu verzichten! Also wozu soll ich die AGBs lesen, selbst wenn ich sie verstünde?“

Vor Gefahren, die man nicht erkennt, kann man sich auch nicht schützen

Das Dilemma, dem vermutlich auch die meisten der Gehackten erlegen sind, ist: Entweder man hat es bequem und tut, was die Anbieter verlangen, nämlich „akzeptieren, zustimmen, einwilligen“, auch, wenn man gar nicht weiß worein genau, oder aber man kann Dienste und Webseiten nicht benutzen. Um da nicht der Bequemlichkeit nachzugeben müsste man wissen, welche Folgen das haben kann. Da die Allgemeinen Geschäftsbedingungen (AGB) und die Datenschutzerklärung häufig von Juristen verfasst werden, versteht der Laie meistens wenig, selbst, wenn er sich durch die langen Texte hindurch quälen würde. Paypal hatte mal 80 Seiten und wurde deswegen im Netz veräppelt. Bei anderen Firmen darf man sich die Texte in der eigenen Sprache aus einem Wust von Texten heraus suchen.

AGBs und Datenschutzerklärungen dienen dazu den Anbieter von möglichst viel Haftung zu befreien und ihm gegenüber dem Endverbraucher eine bessere rechtliche Position zu verschaffen. Sonst könnte man es ja zumindest im Lande bei den Regeln des Bürgerlichen Gesetzbuches belassen. Da aber viel Firmen international tätig sind, versuchen sie mit Hilfe der AGBs sich so weit wie möglich abzusichern. Bei Apple bekommt man z.B. beim iPad in kleinster hellgrauer Schrift: „Einjährige beschränkte Apple-Garantie-Zusammenfassung“, obwohl in der EU eine zweijährige Garantie verlangt wird.

All das erklärt schon ein wenig, weshalb die vom Datendiebstahl Betroffenen vielleicht gar nicht so leichtsinnig waren, wie man auf den ersten Blick meinen könnte. Sie dürften in vielen Fällen auf die Lektüre und das Verstehen und Durchdenken des Gelesenen bei AGBs und Datenschutz-Erklärungen verzichtet haben, vielleicht auch, weil: „Das machen doch alle so!“ Aber wie soll man sich vor einer Gefahr schützen, die man gar nicht kennt?

Und man muss das Kleingedruckte ja nicht nur einmal lesen, sondern für jedes benutzte Programm und häufig nach einem „Update, Upgrade, Patch“ also fast nach jeder Änderung eines Programmes oder des Betriebssystems. Eigentlich müsste man jedes Mal vergleichen, was in dem steht, dem man bereits zugestimmt hat und worin sich das neue „Kleingedruckte“ davon unterscheidet. Wenn dafür im Monat eine Stunde reichen würde, wäre das vermutlich recht flott.

Vielfalt macht Unübersichtlich

Die Digitalisierung hat Vieles, wofür man früher ein eigenes Gerät brauchte, in Rechner und Smart-Phones integriert:

- Fotoapparat, Filmkamera, Dunkelkammer (Fotobearbeitung), Schneidetisch (für Filme)
- Mikrophon, Aufzeichnungsgerät (Tonband, Cassette, CD etc.), Abspielgerät (Plattenspieler, Tonband, CD-Player, MP3-Player), Wiedergabegerät (Radio, Hifi-Anlage)
- Fernseher samt Speichermöglichkeit (Video, DVD)
- Rechner samt Grafischer Darstellung (Kurven, Tabellen)
- Schreibmaschine samt Korrekturhilfe und Speicher, Diktiergerät, Notizblock, Zeichenblock, Bücherregal (für elektronische Bücher)

- Nachschlagwerk (Duden, Lexikon, Sprachwörterbücher)
- Kommunikationsmittel (Telefon, Fax (heute via E-mail), E-mail, SMS, Internet, Videotelefonie, Twitter, etc.)
- Ortung (Kompass, GPS, Maßband, Karten, Navigationsgerät)
- Schnittstelle zu verschiedenen Kommunikationswegen (Bluetooth, Wifi, Kabel und Router)
- Darstellung von Kommunikationsinhalten (SMS, E-mail, Internet, Dienste für bestimmte Interessen, z.B. Filme, Fotos, Benachrichtigungen; ggf. so genannte „Soziale Medien“, also Benutzergruppen)
- Taschenlampe
- Zahlungsmittel und Mittel um Bankgeschäfte zu tätigen
- Medien, wie die Tageszeitung, die man ebenfalls mit Hilfe des Gerätes lesen könnte.

Diese unvollständige Liste, die durch geeignete Programme (Apps von „application“, also Anwendung) erweitert wird, zeigt schon, dass die wenigsten Mitbürger früher alle diese Geräte beherrscht hätten. Es ist daher kein Wunder, wenn Viele sich von der Vielfalt der Möglichkeiten überfordert fühlen und auch nicht alle nutzen. Die Symbole der Apps lassen sich aber häufig nicht vom Bildschirm tilgen, so dass sie schon dort für Unübersichtlichkeit sorgen.

Selbstverständlich müsste man bei einem neuen Gerät auch sämtliche Einstellungen überprüfen und an die eigenen Bedürfnisse anpassen. Bei einem iPad sind das erst einmal über 40 Anwendungen, die man in ihren Fähigkeiten und möglicher Gefährlichkeit zunächst überhaupt nicht einschätzen kann. Hinzu kommen jene Daten, die das Gerät braucht, um Verbindung zu den verschiedenen Diensten aufbauen zu können, also Telefonnummern, E-mail-Adressen, die Daten des Anbieters, falls man einen anderen nutzen möchte, als eigentlich vorgesehen (Bei einem Smart-Phone geht man meistens über den Anbieter des Telefonvertrages ins Netz. Will man einen anderen Anbieter nutzen, sind weitere Einstellungen nötig.)

Es ist daher kein Wunder, dass viele Leute die Übersicht verlieren, oder zumindest nicht in jedem Fall wissen, welche Einstellungen sie wählen müssten, um sicher zu sein. In vielen Fällen dürfte allein die Vielfalt der gebotenen Möglichkeiten die Benutzer überfordern, so dass sie unsicher sind (und deshalb die Werkseinstellungen vorsichtshalber mal nicht ändern). Und wenn man unsicher ist, dann macht man eher Fehler, die bei derartigen Geräten die Sicherheit der Daten gefährden können.

Troy Hunt, ein australischer Mitarbeiter von Microsoft, hat nun eine Sammlung von 773 Millionen geknackten E-mailadressen und deren Passwörter öffentlich gemacht und fand darunter auch seine eigenen, aber zum Glück veralteten Daten. 773 Millionen, das ist mehr als Europa Einwohner hat! Wenn es noch eines Beweises bedurft hätte, dass das Knacken von E-mail-Adressen und deren Passwörtern von einigen Leuten als Sport betrieben wird und man als Einzelner ziemlich hilflos ist, hier ist er. Der größte Datenklau waren wohl die 3 Milliarden Nutzerdaten, die bei Yahoo „abgegriffen“ wurden.

Troy Hunt betreibt auch eine englische Webseite Have I Been Pwned, auf der man seine E-mail-Adresse kostenlos darauf überprüfen lassen kann, ob sie gehackt wurde. Ungefähr jeder Dritte der 2,2 Millionen Nutzer war auch in diesem Datenberg von über 87 GB zu finden, also gehackt. Und man muss bedenken, dass diese Webseite wohl eher von denen aufgerufen wird, die sich des Risikos bewusst sind und es zu verringern versuchen. Man darf also davon ausgehen, dass im Alltag mehr als jede dritte E-mail-Adresse gehackt und das Passwort entschlüsselt wurde!

Es gibt auch eine deutschsprachige Webseite beim Hasso-Plattner-Institut der Universität Potsdam, die Ähnliches leistet: https://sec.hpi.uni-potsdam.de/ilc/search.

Es ist falsch zu glauben, dass irgend wann einmal alle Menschen anständig wären, so dass man auf Sicherheitsmaßnahmen verzichten könnte. Daher sollte man grundsätzlich so wenig Daten, wie möglich ins Internet stellen (z.B. bei E-mail, Webseiten besuchen, Käufe tätigen oder Dienstleistungen buchen). Anbieter sollten darauf achten, dass sie nur solche Daten abfragen, die im konkreten Fall wirklich notwendig sind. Sensible Daten sollte man - wenn irgend möglich - auf einem Gerät speichern, dass keine Verbindung zum Internet hat. Das alles ist allerdings mühsamer, als wenn man ein Gerät mit den Werkseinstellungen benutzt, die darauf ausgerichtet sind es dem Nutzer so bequem wie möglich zu machen.

Die Entscheidung, ob man die Bequemlichkeit höher einschätzt, als die Sicherheit der eigenen und, im Falle eines Angriffes, vielleicht auch der Daten anderer muss man selbst treffen. Es wäre allerdings wünschenswert, wenn die Hersteller der Geräte und die Anbieter von Diensten die Nutzer dabei nicht nur mit langen Texten zum Datenschutz informieren („Wir nehmen Datenschutz sehr ernst...), sondern die Gestaltung von Geräten und Diensten so vorzunehmen, dass es ganz einfach ist, sich sicherer im Netz zu bewegen.

Solange aber die großen Firmen mit den Daten, die sie von Nutzern erbeuten, oder dank des Kleingedruckten vielleicht auch legal erwerben, Milliarden verdienen, darf man davon ausgehen, das genau dies nicht geschehen wird. Facebook soll nach einer Berechnung pro Nutzer und Monat etwas 5 € verdienen. Google hat erst kürzlich 20 Milliarden in einem Steuerparadies „geparkt“. Das zeigt, solche angeblich kostenlosen Dienste sind Gelddruckmaschinen, die obendrein die Umwelt belasten, weil man für das Internet und alle daran angeschlossenen Geräte große Mengen von elektrischem Strom braucht. Wer also sparsam mit Daten im Netz umgeht, der schont auch ein klein wenig die Umwelt. Und wenn das Millionen tun, sind das ganz erhebliche Mengen, die wir entweder direkt (über die Stromrechnung) oder indirekt über Umweltschäden bezahlen.