Der IT-Experte **Wolfgang Romey** beschreibt hier die Untiefen und Abgründe, die sich in der modernen Telekommunikation aufgetan haben. Auch wenn man das ganze Thema eher gelassen sehen wollte, so ist doch die Frage zu stellen, ob es klug ist, sich in diesem Bereich auf Quasi-Monopole zu verlassen, noch dazu, wenn diese fast alle aus nur einem Staat stammen, der zurzeit seine „wir zuerst"-Politik auf die Spitze treibt. Dadurch, dass diese Entwicklung schon sehr weit fortgeschritten ist und weiter fortschreitet, wird eine Umstellung bzw. Abnabelung natürlich immer schwieriger und ist mit erheblichen Kosten und Aufwand verbunden, vor denen viele auch verständlicherweise zurückschrecken. Aber man sollte zumindest mit einer Einschätzung der individuellen IT-Lage nicht warten, bis eine mögliche Umstellung noch schwieriger geworden ist. Wenn in Bildungseinrichtungen ein Anfang gemacht würde, wäre das ein Schritt in eine gute Richtung. Diese Einleitung ist von **Moritz Müller**.

Nichts zu verbergen von Wolfgang Romey

„Ich habe nichts zu verbergen", ist das Argument, das häufig genannt wird, wenn man darauf hinweist, dass im digitalen Raum persönliche Daten umfassend abgeschöpft und insbesondere für Werbung und Profilbildung, aber auch für Überwachung aufbereitet und eingesetzt werden. Eine aktuelle Studie hat belegt, dass die Werbeindustrie Daten umfassend abschöpft und dabei systematisch rechtswidrig handelt.

Dass die Leute ernsthaft der Meinung sind, dass ihre persönliche E-Mail-Korrespondenz, ihre Gesundheitsdaten, Vertragsdaten oder Zugangsdaten zu Bankkonten nicht schützenswert sind, ist schwer zu glauben. Weist man darauf hin, erhält man oft die Antwort, dass die Daten doch sowieso schon erfasst seien und man dagegen nichts machen könne. Wenn man fahrlässig mit seinen Daten umgeht, ist das durchaus richtig; aber auch kein Wunder.

Was diese Menschen aber nicht bedenken, ist, dass der leichtfertige Umgang mit ihren persönlichen Daten auch andere betrifft. Einfache Beispiele sind die Nutzung des Google-Email-Dienstes Gmail, bei dem der Inhalt aller eingehenden E-Mails von Google erfasst und die Adresse gespeichert werden, oder das Auslesen vollständiger Adressbücher beispielsweise durch WhatsApp, wodurch die eigenen Adressdaten dort landen und beispielsweise an Facebook weitergegeben werden.

Überraschend ist, dass auch Menschen mit ihren Daten fahrlässig umgehen, die es eigentlich besser wissen müssten! Das sind alle Menschen, die eine kritische Haltung zum politischen System einnehmen oder politisch aktiv sind und beispielsweise an Demonstrationen teilnehmen, auf kritischen Organen veröffentlichen, Mitglieder von

politischen Parteien oder Gruppen sind. Die Gefahr, dass diese Menschen das Interesse von Überwachungsdiensten erwecken, ist real. Die hier beschriebenen Überwachungsmöglichkeiten betreffen insbesondere diese Menschen. Da die Überwachung verdeckt erfolgt, ist nur zum Teil bekannt, wie weit sie schon in der Realität eingesetzt werden.

Sehen diese Menschen kein Problem darin, dass über die Adressbücher in Verbindung mit der Erfassung des Standortes ermittelt werden kann, wer zu einer politischen Gruppe gehört und wer wann an welchen Aktivitäten wie Gruppentreffen oder Demonstrationen teilgenommen hat? Ist es nicht beunruhigend, wenn man weiß, dass der Inhalt einer E-Mail-Korrespondenz einer Gruppe abgegriffen werden kann; also beispielsweise der Inhalt von Einladungen?

Ist es in Ordnung, dass die Gefahr besteht, dass der Inhalt von Texten wie Protokollen, Beschlussvorlagen oder politischen Artikeln wenigstens teilweise erfasst werden kann und die allermeisten Aktivitäten am Rechner an Microsoft weitergeleitet werden, wenn Microsoft-Office auf einem Rechner genutzt wird, der unter Microsoft-Windows läuft? Verantwortlich ist der auf den Windows-10-Rechnern laufende Dienst Cortana. Was leider kaum bekannt ist – man kann diesen Dienst auch deaktivieren.

Das Smartphone ist wohl das digitale Gerät, mit dem eine Ausforschung der Nutzer am umfassendsten möglich ist und, wie unter anderem die Snowden-Enthüllungen belegt haben, geschieht. Es ist fast immer dabei, oftmals online, die Ortungsfunktion ist eingeschaltet und es wird auch auf Veranstaltungen für Ton, Bild oder Filmaufnahmen genutzt. Der Umgang mit dem Smartphone ist deshalb wesentlich für den verantwortlichen Umgang mit seinen persönlichen, aber auch den Daten einer Gruppe oder Organisation.

In einem Smartphone stecken eine Fülle von Sensoren, die verschiedene Überwachungsfunktionen, beispielsweise die Erfassung des Standortes auch ohne die eingeschaltete Standortfunktion, möglich machen. Will man sich dagegen wehren, reicht es nicht, das Smartphone auszuschalten, es muss auch der Akku entfernt werden, was nur noch bei wenigen Geräten wie dem FairPhone möglich ist, das ist ein Skandal für sich. Das wesentliche Verschleißteil kann nicht ersetzt werden!

Dass auch ausgeschaltete Smartphones geortet werden können, ist allerdings nur unter bestimmten Voraussetzungen möglich. Dazu muss auf dem Smartphone bestimmte Software installiert sein. Diese Software kann beispielsweise durch die Polizei oder Geheimdienste installiert werden. Einfacher ist aber, sie über eine App unterzuschieben, die eine andere Funktion vorgibt, vielleicht ein Spiel, und im Hintergrund unbemerkt die

Überwachungssoftware installiert und ausführt. Das Unterschieben von versteckten Funktionen wie Ortung oder Auslesen der Adressdaten ist durchaus verbreitete Praxis, beispielsweise bei Taschenlampen-Apps. Für eingeschaltete Smartphones gibt es übrigens eine Reihe von Spionageprogrammen, die auch von Privatleuten genutzt werden können. Die Beschreibung einiger Programme findet sich hier. Der Funktionsumfang ist erschreckend.

Ein kaum vermeidbarer Teil des entstehenden Datenschattens von Personen sind die Adressdaten. Für eine Gruppe reicht es, dass einige auf ihrem Smartphone Apps wie beispielsweise WhatsApp nutzen, die das Auslesen des auf dem Gerät vorhandenen Adressbuches fordern. Wenn die Adressbücher der Teilnehmer abgeglichen werden, ist man schon recht nah an der Zusammensetzung der Gruppe. Die Adressdaten bei den Ausforschungs-Unternehmen können übrigens Jahrzehnte zurückreichen, da auch Daten von Fluggesellschaften, Reisebüros und Bestellungen von vor der Zeit des Internets gesammelt wurden und werden. Werden auch die persönlichen Kalender und die Standortdaten beispielsweise über Google-Maps abgeglichen, können die Zusammensetzung einer politischen Gruppe und ihre Aktivitäten sehr weit erschlossen werden.

Umfassender wird das Bild der Zusammensetzung der Gruppe, wenn etwa bei einer Demonstration fotografiert wird. Werden die Bilder zeitnah in ein sogenanntes soziales Netzwerk hochgeladen, muss man davon ausgehen, dass dort versucht wird, die Person zu erkennen, auch in Verbindung mit den schon vorhandenen Daten, beispielsweise bei Facebook der angeblichen Freunde. Gelingt die Erkennung nicht, werden die Bilder in die riesige Bilder-Datenbank von Facebook zur späteren Verwendung eingepflegt. Es ist seit Snowden bekannt, dass Facebook und auch Microsoft mit der NSA zusammenarbeiten. Es kann also nicht überraschen, wenn diese Bilder in den Datenbanken für die Überwachung durch die Polizeibehörden landen.

Auch Microsoft ist in diesem Feld aktiv. Bei der Verwendung einer App, die für Sehbehinderte gedacht ist, ist deutlich geworden, dass Microsoft die Bilder dazu nutzt, um biometrische Datenbanken zur Gesichtserkennung aufzubauen. „Als wir die App mit alten Fotos ausprobierten, gab sie bei manchen Personen gleich den Namen aus.“ Auch Facebook bietet eine ähnliche Funktion an.

Dass die Gefahr real ist, ist in den letzten Tagen sichtbar geworden. „Eine bislang kaum bekannte US-Firma hat einem Bericht der New York Times zufolge rund drei Milliarden Bilder von Menschen aus dem Internet zusammengestellt, um eine umfassende Datenbank zur Gesichtserkennung zu entwickeln. Im vergangenen Jahr sei der Zugang dazu mehr als 600 Behörden als Service angeboten worden“, schrieb die Zeitung am 18. Januar 2020 unter

Berufung auf das Unternehmen Clearview AI. Pikant ist, dass Peter Thiel einer der Geldgeber der Firma ist. Er hat auch Anteile an Facebook, das in den Nutzungsbedingungen das Abgreifen von Bildern untersagt.
Anm. MM: *Siehe hierzu auch gestern auf den NachDenkSeiten.*

Das wird aber nicht von allen als Problem empfunden. So finden sich auf Instagram, also bei einem Arm der Datenkrake Facebook, reichlich Fotos von Teilnehmern an den Fridays-For-Future-Demonstrationen. Ob das für eine spätere Bewerbung günstig oder ungünstig ist, wird sich zeigen.

Besonders tückisch sind die digitalen Assistenten, die auf die Eingabe eines gesprochenen Aktivierungsbefehls warten und deshalb ununterbrochen die Gespräche mithören und, wie man inzwischen sicher weiß, auch aufzeichnen und auswerten; bisher durch Menschen, zukünftig aber auch automatisch. Diese Gefahr hat sich inzwischen über Ausforschungsgeräte wie Alexa auch in die Privathaushalte eingeschlichen. Man sollte immer darauf drängen, dass derartige Geräte abgeschaltet werden, sonst landet die eigene Stimme in einer Datenbank, Gesprächsinhalte werden erfasst und ausgewertet.

Das Bild der Zusammenhänge, in denen man sich bewegt, wird so immer umfassender und bei politisch aktiven Menschen immer gefährlicher. Selbstverständlich werden die Stimmdaten mit vorhandenen anderen Daten zusammengeführt, sodass sich ein immer komplexerer Datenschatten der jeweiligen Personen und, das ist wichtig, ihrer Zusammenhänge ergibt. Da auch die inhaltliche Erkennung von Sprache wie die Gesichtserkennung schnell Fortschritte machen, muss man davon ausgehen, dass mindestens in naher Zukunft, wenn nicht schon heute, Ort, Zeit, Teilnehmer und Gesprächsinhalte bei einer Veranstaltung erfasst und ausgewertet werden. Smartphones haben deshalb bei politischen Veranstaltungen in der Regel nichts zu suchen.

Es wäre noch eine Reihe von Bereichen anzusprechen, in denen man sorgfältig mit seinen persönlichen Daten umgehen muss, wie etwa die sogenannten sozialen Netzwerke. Aus Platzgründen sollen hier nur noch zwei davon behandelt werden: der Umgang mit E-Mails und die Verwendung von Windows-Rechnern.

Wenn man nicht will, dass die Inhalte von E-Mails, die ja durchaus interessant für die „Dienste“ sein können, unter anderem durch Windows 10 Cortana erfasst werden, muss man seine E-Mails zwingend verschlüsseln; sonst sind sie öffentlich wie eine Postkarte. Verschlüsselung gilt als schwierig einzurichten und zu nutzen. Beides gilt nicht mehr. Zur Einrichtung gibt es eine Reihe leicht verständlicher Anleitungen, unter anderem hier. Die Nutzung ist nach kurzer Zeit einfach. Dass versucht wird, das Bild der schwierigen Nutzung

aufrechtzuerhalten, soll Menschen von der Nutzung abhalten. Politisch denkende und handelnde Menschen verhalten sich leichtfertig, wenn sie sich dadurch abschrecken lassen. Partner für verschlüsselte E-Mails finden sich schnell, wenn man mit der Verschlüsselung beginnt.

Leichtfertig gehandelt wird auch, wenn beispielsweise von publizistisch tätigen Menschen gefordert wird, Texte, die veröffentlicht werden sollen, als Microsoft-Word-Datei einzureichen. Dass die Bearbeitung dann in der Regel auf Rechnern mit dem Betriebssystem Microsoft Windows erfolgt, hat zur Folge, dass die bei der Erstellung von Texten anfallenden Daten umfassend erfasst werden können. Das gilt nicht nur für den eigentlichen Text: die dazu gehörenden Recherchen, damit verbundene Korrespondenz, Vertragsdaten, alles kann erfasst werden. Besonders kritisch ist das, wenn der Text auf verdeckt ermittelten Informationen beruht und gegebenenfalls Whistleblower geschützt werden müssen. Alles, was in irgendeinem Format in den Windows-Rechner eingegeben wird, ist gefährdet.

Warum ist das möglich? Es inzwischen durch mehrere Untersuchungen gesichert, dass das aktuelle Microsoft-Betriebssystem Windows 10 sich nicht vollständig dagegen absichern lässt, dass Daten, die bei der Nutzung anfallen, an Microsoft übertragen werden.

> „Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und das niederländische ‚Autoriteit Persoonsgegevens' sowie das Bundesamt für Sicherheit in der Informationstechnik haben diese Problematik untersucht und sind zu dem Ergebnis gekommen, dass eine vollständige Übertragung mit systembasierten Abhilfemaßnahmen allein nicht verhindert werden kann. Auch netzwerkbasierte Abhilfemaßnahmen scheinen nur über den Umweg, eine direkte Internetanbindung von Windows-10-Systemen zu unterbinden und den Internetzugang (über Browser oder Fachanwendungen) über eine Virtualisierungs- oder Terminallösung erfolgen zu lassen, noch erfolgversprechend."

Auf Wikipedia findet man: Windows 10 überträgt „eine Vielzahl von Daten an Microsoft. Für den Sprachassistenten Cortana nutzt Microsoft z. B. den Kommunikationsverlauf und die Inhalte von Nachrichten. Außerdem werden unter anderem folgende Informationen verwendet: Standortinformationen und -verlauf des Geräts, Kontakte, Spracheingaben, Suchverlauf, Kalenderinformationen. Diese Informationen werden auf einem Microsoft-Server im Internet gespeichert. Die übertragenen Daten umfassen außerdem eine

appübergreifende Werbe-ID, mit der es möglich ist, einen Benutzer bei der Benutzung unterschiedlicher Apps eindeutig zu identifizieren und ihm personalisierte Werbung anzuzeigen, sobald er Seiten im Internet aufruft. Übertragen werden außerdem nicht näher benannte Informationen zum Schreibverhalten und Informationen zur Standortbestimmung (z. B. über WLANs in der Umgebung). Außerdem gewährt Windows 10 vielen Apps standardmäßig Zugriff auf Webcam und Mikrofon." Es ist nicht zu prüfen, welche Daten davon an Microsoft weitergeleitet werden und was dann mit den Daten geschieht. Damit ist alles, was in irgendeinem Format in den Windows-Rechner eingegeben wird, potenziell gefährdet. Um die Gefahr zu verringern, muss man sich schon sehr intensiv mit den Telemetrie-Einstellungen von Windows 10 auseinandersetzen und viele Funktionen ausschalten. Wie die Untersuchungen gezeigt haben, ist ein vollständiger Schutz aber nicht möglich.

Auch aus einer Untersuchung für die Bundesverwaltung ergibt sich, dass die Abhängigkeit von Microsoft zu groß ist. Einer der in der Untersuchung formulierten Schmerzpunkte (!) lautet: „Eingeschränkte Informationssicherheit: Aufgrund des nicht einsehbaren Quellcodes hat die Bundesverwaltung nur eingeschränkte Möglichkeiten, die Informationssicherheit von Microsoft-Software zu überprüfen. So enthalten neue Produktversionen Telemetriekomponenten, die Metadaten erfassen und sammeln. Dabei werden Daten auf Microsoft-Server übertragen und gespeichert, die in der Folge an U.S.-Behörden gelangen könnten."

Trotz entsprechender Forderungen hat sich bis heute sehr wenig daran geändert. Dadurch, dass Microsoft die Nutzer in die Cloud zu lockt – dort können das Office-Paket online genutzt und die Daten gespeichert werden – verschlechtert sich die Situation immer weiter. Es ist weder bekannt noch kontrollierbar, welche Software in der Microsoft-Cloud läuft und welche Aufgaben sie erledigt. Zudem haben die US-Behörden Zugriff auf die Daten, die außerdem jederzeit verloren gehen können, wie es Nutzern von Adobe in Venezuela gegangen ist, deren Nutzerkonten ohne Vorankündigungen gesperrt wurden.

Ist man hilflos dagegen? Nein! Im Internet gibt es eine Reihe von Seiten zur sogenannten „Digitalen Selbstverteidigung" wie beispielsweise die von dem Blog Netzpolitik herausgegebene Broschüre, die über Möglichkeiten aufklären, verantwortungsvoller mit seinen persönlichen Daten, aber auch mit den Daten einer Organisation oder eines Publikationsorgans umzugehen.

Sich von Windows und Word zu verabschieden, ist leider nicht ganz einfach, aber möglich. Statt die Überwachungssoftware von Microsoft zu verwenden, kann man das quelloffene, lizenzkostenfreie Betriebssystem Linux und die mitgelieferte freie Software verwenden.

Schwierig scheint das, weil neue Rechner schon lange mit vorinstalliertem Windows ausgeliefert wurden und noch werden. So haben fast alle Nutzer noch nie ein neues Betriebssystem installiert. Der Installationsprozess für Linux ist zwar inzwischen einfach geworden, ohne Begleitung fühlen sich die meisten Nutzer aber überfordert. Informationen gibt es reichlich im Netz, beispielsweise hier.

Eine zweite Schwierigkeit ist, dass es nicht „das“ Linux gibt. Auf der Seite „distrowatch“ kann man fast 300 Versionen, sogenannte Distributionen, finden. Der Vorteil für den Nutzer ist, dass er aus einer großen Zahl seine Auswahl treffen kann und auch Versionen für spezielle Bedürfnisse wie Multimedia oder Grafik, Bildung oder Wissenschaft finden kann. Zunächst erschlägt diese Vielfalt die normalen Nutzer, eine Anfrage im Netz grenzt die die Auswahl aber meistens schnell ein. Ein weiterer Vorteil ist, dass die Entwicklung von Viren für Linux durch die Vielfalt deutlich behindert wird und Linux auch deshalb deutlich sicherer als Windows ist. Genannt werden soll hier noch der Aspekt der Nachhaltigkeit: Nach einer Installation von Linux ist der Rechner meist deutlich schneller als unter Windows, sodass er wesentlich länger genutzt werden kann. Eine Neuanschaffung kann in der Regel mehrere Jahre hinausgeschoben werden.

Für die Erledigung der gängigen Aufgaben (Textverarbeitung, Tabellenkalkulation, E-Mail) gibt es leistungsstarke Software, die laufend weiterentwickelt wird und kostenfrei zu haben ist. Mit dieser Software kann wenigstens teilweise auch der bisherige Workflow beibehalten werden. Hilfe zu vielen Fragen ist in der Regel im Internet zu finden. Warum also nicht den Schritt weg von Windows wagen und so der Ausforschung der eigenen Person und der Gruppen, in denen man arbeitet, ein Stück Einhalt gebieten und damit der Verantwortung, die man für sie trägt, besser gerecht werden?

Titelbild: Shutterstock/ Mykola Komarovskyy