Löse dein Problem mit einem Augenzwinkern

Die App fragt nach meiner Gesundheit, ich frage nach meiner Privatsphäre

Wie du Gesundheits-Apps bewusst nutzt und die Menge deiner preisgegebenen persönlichen Daten begrenzt



Max Paradox

Die App fragt nach meiner Gesundheit, ich frage nach meiner Privatsphäre

Wie du Gesundheits-Apps bewusst nutzt und die Menge deiner preisgegebenen persönlichen Daten begrenzt

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384904879

ALL-IN Rafał Płonkowski



INHALTSVERZEICHNIS

INTRO 5

Kapitel 1 - Dein Smartphone weiß, wie du schläfst. Aber wer weiß es noch? 12

Kapitel 2 - Kostenlose App, äußerst persönliche Währung 23

Kapitel 3 - „Alles erlauben“ oder wie du die Schlüssel zu deiner digitalen Wohnung abgibst 35

Kapitel 4 - Ein Vorhängeschloss auf dem Bildschirm macht eine App noch lange nicht heilig 46

Kapitel 5 - Alles mit allem verbunden: Das digitale Spinnennetz deiner Gesundheit 57

Kapitel 6 - Benachrichtigungen, Erinnerungen und andere Formen digitaler Neugier 69

Kapitel 7 - Standardeinstellungen oder Privatsphäre nach den Vorstellungen des Herstellers 80

Kapitel 8 - Du musst der App nicht die gesamte Geschichte deines Körpers erzählen 91

Kapitel 9 - Bevor du auf „Installieren“ tippst, stell ein paar Nachforschungen an 102

Kapitel 10 - Die ersten fünfzehn Minuten mit der App: Richte sie nach deinen Bedürfnissen ein 113

Kapitel 11 - Deine Daten wollen verreisen. Wie bereitest du sie auf eine sichere Reise vor? 124

Kapitel 12 - Digitaler Frühjahrsputz: Wie du Daten löschst, die einfach nicht ausziehen wollen 136

Kapitel 13 - Ich teile meine Ergebnisse, nicht mein ganzes Leben. Wie du Gesundheitsdaten nach deinen eigenen Regeln weitergibst 147

Kapitel 14 - Was tun, wenn etwas schiefgeht? Ruhig auf ein Datenproblem reagieren 159

Kapitel 15 - Wenn die App notwendig ist, obwohl die Privatsphäre „Nein“ sagt 170

Kapitel 16 - Wenn andere deine Daten haben wollen: Arbeitgeber, Versicherer und die familiäre Gesundheitskommission 182

Kapitel 17 - Ich habe keine Zeit für Datenschutz. Wie du deine Daten schützt, wenn das Leben nicht mitspielt 195

Kapitel 18 - Privatsphäre auf Autopilot, aber mit der Hand am Steuer 207

Kapitel 19 - Warnsignale, die du erkennen solltest, bevor deine Privatsphäre wieder Urlaub macht 219

Kapitel 20 - Meine Gesundheit, meine Daten, meine Regeln 232

INTRO

Es ist 7:14 Uhr morgens. Dein Smartphone teilt dir mit, dass du sechs Stunden und zweiunddreißig Minuten geschlafen hast, wobei dein Tiefschlaf verdächtig kurz ausgefallen ist. Deine Smartwatch empfiehlt dir Ruhe, die Ernährungs-App erinnert dich ans Frühstück, und eine Anwendung zur Überwachung deines Wohlbefindens möchte wissen, ob du dich ängstlich fühlst. Du hast noch nicht einmal deinen zweiten Hausschuh gefunden, und schon haben drei Geräte ihre Meinung über deinen Körper abgegeben. Ein viertes bittet gerade um Zugriff auf deinen Standort. Offenbar hängt deine Flüssigkeitsversorgung von deinen geografischen Koordinaten ab.

Alles sieht ganz harmlos aus. Bunte Diagramme, freundliche Benachrichtigungen, sympathische Symbole und das Versprechen, den eigenen Körper besser kennenzulernen. Gesundheits-Apps können tatsächlich sehr nützlich sein. Sie helfen dabei, an die Einnahme von Medikamenten zu denken, körperliche Aktivitäten zu beobachten, den Schlaf zu analysieren, ein Symptomtagebuch zu führen oder Informationen für einen Arzttermin zusammenzustellen. Das Problem beginnt, wenn wir für ein bisschen Bequemlichkeit wesentlich mehr Informationen preisgeben, als eigentlich notwendig wäre. Manchmal tun wir das bewusst. Viel häufiger tippen wir auf „Akzeptieren“, weil wir endlich dieses verdammte Diagramm sehen wollen.

Und genau hier taucht eine Frage auf, die sich viel zu wenige Menschen stellen: Was passiert eigentlich mit den Informationen über unsere Gesundheit?

Es geht keineswegs nur darum, ob jemand erfährt, wie viele Schritte wir gemacht haben. Gesundheitsdaten können ein erstaunlich detailliertes Bild unseres Lebens zeichnen. Unsere Schlafgewohnheiten, die Häufigkeit körperlicher Aktivitäten, Veränderungen des Körpergewichts, dokumentierte Symptome, Informationen über den Menstruationszyklus, eingenommene Medikamente oder unsere psychische Verfassung können Dinge offenbaren, die wir nicht unbedingt mit Fremden teilen möchten. Besonders dann, wenn einzelne Informationen mit Gerätekennungen, dem Nutzungsverlauf einer App oder anderen Daten verknüpft werden.

Stell dir vor, du führst ein privates Tagebuch. Darin hältst du fest, wann du dich schlecht fühlst, was dir Sorgen bereitet und welche Veränderungen du an deinem Körper bemerkst. Dann bietet dir jemand ein elegantes Notizbuch an, das selbstständig Diagramme erstellt und dich an regelmäßige Einträge erinnert. Klingt hervorragend. Erst später entdeckst du, dass die Verwendung dieses Notizbuchs damit verbunden sein kann, dass ein Teil deiner Informationen an weitere Unternehmen oder Dienstleister weitergegeben wird. Plötzlich stellt sich heraus, dass dein privates Tagebuch über ein größeres Kontaktnetzwerk verfügt als der Organisator einer internationalen Konferenz.

Natürlich gibt nicht jede Anwendung Daten an Werbetreibende weiter, und allein die Anforderung einer Berechtigung beweist noch keinen Missbrauch. Verschiedene Programme funktionieren unterschiedlich, verfolgen verschiedene Geschäftsmodelle und verwenden unterschiedliche Sicherheitsmaßnahmen. Manche speichern Informationen hauptsächlich auf dem Gerät, andere synchronisieren sie mit Servern, und wieder andere nutzen

die Dienste externer Anbieter. Gerade deshalb lohnt es sich, diese Unterschiede erkennen zu lernen, anstatt sämtliche Apps wie verdächtige Teilnehmer einer Eigentümerversammlung zu behandeln.

Bequemlichkeit hat ihren Preis, aber du musst nicht immer mit deinen Daten bezahlen

Über die Jahre haben wir uns daran gewöhnt, dass digitale Bequemlichkeit bedeutet, möglichst schnell eine Benachrichtigung nach der anderen zu bestätigen. Du möchtest eine App installieren? Erstelle ein Benutzerkonto. Du möchtest deine Statistiken sehen? Aktiviere die Synchronisierung. Du möchtest Erinnerungen erhalten? Erteile die entsprechenden Berechtigungen. Du möchtest endlich weitermachen? Lies bitte zunächst ein Dokument, dessen Sprache vermutlich bei einer Meisterschaft im Verkomplizieren einfacher Sätze entwickelt wurde.

Infolgedessen treffen wir viele Entscheidungen vollkommen automatisch. Nicht, weil uns unsere Privatsphäre gleichgültig wäre, sondern weil uns die Zeit, die Informationen oder schlicht die Geduld fehlen. Es ist schließlich schwierig, jede einzelne Einwilligung gründlich zu analysieren, wenn man eigentlich nur überprüfen wollte, ob der gestrige Spaziergang tatsächlich vierzig Minuten gedauert hat. Die Entwickler von Benutzeroberflächen wissen sehr genau, dass ein Mensch, der von immer neuen Dialogfenstern erschöpft ist, vor allem eines möchte: die Einrichtung endlich abschließen.

Das bedeutet allerdings nicht, dass du dich zwischen einem vollständigen Verzicht auf Technologie und der Preisgabe sämtlicher Informationen entscheiden musst. Es gibt zahlreiche vernünftige Zwischenlösungen. Du kannst nützliche Funktionen verwenden und gleichzeitig den

Umfang der gesammelten Daten begrenzen, Berechtigungen überprüfen, selbst über die Speicherung deiner Informationen entscheiden und auf Funktionen verzichten, die du tatsächlich nicht benötigst.

Entscheidend ist ein Perspektivwechsel. Statt ausschließlich darüber nachzudenken, was eine Anwendung für dich tun kann, solltest du anfangen zu fragen, was sie dafür von dir benötigt. Das erscheint zunächst wie ein kleiner Unterschied, kann aber deine Entscheidungen grundlegend verändern.

Wenn ein Programm, das dich ans Wassertrinken erinnern soll, Zugriff auf deine Kontakte verlangt, darfst du durchaus fragen, warum es die Telefonnummern deiner Freunde braucht. Vielleicht gibt es eine soziale Funktion, die eine solche Anfrage rechtfertigt. Vielleicht ist die Berechtigung freiwillig. Vielleicht funktioniert die Anwendung aber auch ohne sie vollkommen problemlos. In jedem Fall lohnt es sich, die Antwort herauszufinden, bevor du automatisch allem zustimmst.

Privatsphäre bedeutet nicht, in einer digitalen Höhle leben zu müssen

Bei Gesprächen über Datenschutz begegnen uns häufig zwei extreme Ansichten. Die erste besagt, dass es ohnehin keinen Grund zur Sorge gibt, weil „die sowieso schon alles über uns wissen“. Die zweite legt nahe, dass die einzige sichere Lösung darin besteht, Smartphone, Smartwatch und Internet aufzugeben, vorzugsweise in Gesellschaft einiger Kerzen und eines selbst gebastelten Abakus.

Beide Sichtweisen helfen uns herzlich wenig.

Nur weil bestimmte Informationen bereits irgendwo weitergegeben wurden, bedeutet das nicht, dass zukünftige

Entscheidungen keine Rolle mehr spielen. Und es ist auch nicht notwendig, sich vollständig aus der digitalen Welt zurückzuziehen, um die eigene Privatsphäre zu verbessern. Vielmehr geht es darum, unnötige Datenübertragungen bewusst einzuschränken und Kompromisse zu wählen, die zu deinen tatsächlichen Bedürfnissen passen.

Für einen Menschen kann es besonders wichtig sein, seine Symptomgeschichte ausschließlich lokal auf seinem Gerät zu speichern. Jemand anderes entscheidet vielleicht, dass die Synchronisierung zwischen Smartphone und Smartwatch die dafür notwendige Weitergabe bestimmter Informationen wert ist. Wieder jemand anderes braucht die Möglichkeit, Gesundheitsdaten unkompliziert für seinen Arzt zu exportieren. Keine dieser Entscheidungen muss grundsätzlich falsch sein. Entscheidend ist, ob du die Konsequenzen verstehst und ob du die Entscheidung tatsächlich selbst triffst.

Dabei solltest du auch bedenken, dass Privatsphäre und Sicherheit nicht genau dasselbe sind. Eine Anwendung kann gespeicherte Informationen hervorragend schützen und trotzdem mehr Daten sammeln, als du preisgeben möchtest. Umgekehrt kann ein Programm nur wenige Informationen erheben, aber unzureichende Maßnahmen zum Schutz deines Benutzerkontos einsetzen. Wer digitale Anwendungen vernünftig nutzen möchte, sollte beide Aspekte berücksichtigen. Ein kleines Vorhängeschloss auf dem Bildschirm ist schließlich kein magischer Zauberspruch, der sämtliche Probleme verschwinden lässt.

In diesem Buch werden wir deshalb weder digitale Monster jagen noch beweisen wollen, dass jedes Technologieunternehmen heimlich die Kontrolle über deinen Puls übernehmen möchte. Stattdessen beschäftigen wir uns

mit alltäglichen Entscheidungen: der Auswahl einer Anwendung, der Einrichtung eines Benutzerkontos, der Erteilung von Einwilligungen, der Verbindung verschiedener Geräte, der Synchronisierung von Informationen und dem Löschen von Daten, die wir nicht länger speichern möchten.

Du wirst lernen, zwischen Berechtigungen zu unterscheiden, die tatsächlich benötigt werden, und solchen, die du besser hinterfragen solltest. Du wirst verstehen, warum das Entfernen einer App vom Smartphone nicht automatisch bedeutet, dass auch die Informationen in deinem Benutzerkonto gelöscht werden. Außerdem erfährst du, wie du Datenschutzhinweise lesen kannst, ohne vorher noch ein zusätzliches Studium der Rechtswissenschaften und Informatik absolvieren zu müssen.

Nicht alle Antworten werden einfach sein. Manche Funktionen benötigen bestimmte Informationen, und wenn du deren Weitergabe verweigerst, kann das den Komfort oder die Möglichkeiten eines Programms einschränken. Manchmal ist es sinnvoller, Einstellungen zu verändern, manchmal eine andere Anwendung auszuwählen und manchmal einen bewussten Kompromiss einzugehen.

Deine Gesundheit muss kein offenes Buch sein

Eine weitere wichtige Sache sollten wir nicht vergessen. Die Verwendung von Gesundheits-Apps ersetzt keine professionelle medizinische Versorgung. Selbst hochentwickelte Diagramme können ungenau sein, und die automatische Interpretation von Ergebnissen berücksichtigt nicht immer den gesamten gesundheitlichen Zusammenhang. Entscheidungen über Behandlungen und besorgniserregende Symptome erfordern deshalb eine angemessene medizinische Beratung. Gleichzeitig sollten deine Datenschutzeinstellungen nicht verhindern, dass du

deinem Arzt die benötigten Informationen zur Verfügung stellen kannst.

Unser Ziel ist wesentlich bodenständiger: Du sollst wieder mehr Einfluss darauf gewinnen, welche Informationen du weitergibst, an wen und aus welchem Grund.

Dafür musst du kein Experte für Cybersicherheit werden. Du musst auch nicht jedes technische Detail einer Anwendung verstehen. Es reicht, wenn du lernst, die richtigen Fragen zu stellen, Warnsignale zu erkennen und einige konkrete Maßnahmen zum passenden Zeitpunkt umzusetzen.

Denn dein Smartphone darf durchaus wissen, wie viele Schritte du gemacht hast, wie lange du geschlafen hast und wann du zuletzt Sport getrieben hast. Das bedeutet aber noch lange nicht, dass jede Anwendung auf diesem Smartphone einen vollständigen Bericht über dein Leben erhalten muss.

Und wenn dich das nächste Mal ein sympathisches kleines Symbol um Zugriff auf eine weitere Portion persönlicher Informationen bittet, wirst du vielleicht nicht mehr reflexartig auf „Zulassen“ tippen.

Vielleicht fragst du stattdessen zuerst: „Und wozu brauchst du das eigentlich?“

Genau mit dieser Frage beginnt ein bewusster Umgang mit deiner Privatsphäre.

Kapitel 1 - Dein Smartphone weiß, wie du schläfst. Aber wer weiß es noch?

Stell dir vor, du kaufst eine neue Sportuhr. Elegant, leicht und mit so vielen Sensoren ausgestattet, dass sie mit einem zusätzlichen Stethoskop eine kleine Arztpraxis eröffnen könnte. Sie misst deinen Puls, zeichnet deine Aktivitäten auf, schätzt deine Schlafqualität ein und erinnert dich daran, dich zu bewegen. Nach ein paar Tagen betrachtest du sie bereits als deinen persönlichen Berater. Morgens überprüfst du deinen Erholungswert, nachmittags deine Schrittzahl und abends die Zusammenfassung deiner Aktivitäten. Alles sieht wunderbar aus, bis plötzlich eine einfache Frage auftaucht: Wo landen eigentlich all diese Informationen?

Die Antwort ist häufig wesentlich komplizierter, als das kleine Symbol der Anwendung vermuten lässt. Daten können im Speicher des Geräts verbleiben, mit dem Smartphone synchronisiert, an die Server des Diensteanbieters übertragen oder von Unternehmen verarbeitet werden, die bestimmte Funktionen bereitstellen. Ein Teil der Informationen dient möglicherweise ausschließlich dem Betrieb der Anwendung, ein anderer der Analyse ihrer Funktionsweise und in manchen Geschäftsmodellen auch der Personalisierung von Dienstleistungen oder Werbung. Das bedeutet nicht, dass jeder Hersteller auf diese Weise vorgeht. Es bedeutet lediglich, dass der Speicherort der Daten und ihre Verwendung nicht immer auf dem Startbildschirm zu erkennen sind.

Und ausgerechnet diesen Startbildschirm betrachten wir am häufigsten. Ein bunter Kreis zeigt uns, dass wir achttausend Schritte zurückgelegt haben. Herzlichen

Glückwunsch! Unser Körper hat sich bewegt, und die Anwendung hat ihre geometrischen Kenntnisse unter Beweis gestellt. Nur sieht der Nutzer normalerweise nicht, welche technischen Abläufe hinter dieser Messung stehen. Er weiß nicht, welche Informationen lokal gespeichert, welche in die Cloud übertragen wurden und ob die Aktivitätshistorie mit seinem Benutzerkonto verknüpft ist.

Diesen Unterschied zu verstehen, ist der erste Schritt zu einem bewussten Umgang mit Gesundheits-Apps. Du musst dafür nicht die gesamte IT-Infrastruktur des Herstellers kennenlernen. Es genügt zunächst zu verstehen, welche Arten von Informationen bei der täglichen Nutzung entstehen und warum manche davon mehr über dich verraten können, als du ursprünglich angenommen hast.

Daten, die harmlos aussehen

Beginnen wir mit der Schrittzahl. Die Information, dass du an einem bestimmten Tag sechs Kilometer gelaufen bist, erscheint zunächst nicht besonders persönlich. Man könnte sie sogar für langweilig halten. Vor allem, wenn der größte Teil dieser Strecke dadurch entstanden ist, dass du in einem Geschäft nach einem Produkt gesucht hast, dessen Standort offenbar ausschließlich einem Mitarbeiter bekannt ist, der gerade Urlaub macht.

Eine einzelne Messung und eine über viele Monate aufgezeichnete Messhistorie sind allerdings zwei verschiedene Dinge. Die Regelmäßigkeit deiner Aktivitäten kann Hinweise darauf geben, zu welchen Tageszeiten du normalerweise unterwegs bist, wann du dich ausruhst und wie sich deine täglichen Gewohnheiten verändern. Zeichnet die Anwendung zusätzlich deine Route auf, werden die Informationen noch detaillierter. Ein regelmäßig wiederkehrender Ausgangspunkt kann auf deinen Wohnort

hindeuten, während häufige Zwischenstopps Rückschlüsse auf bestimmte Orte ermöglichen, die du besuchst.

Beim Schlaf verhält es sich ähnlich. Die Information über eine einzelne kurze Nacht sagt noch nicht besonders viel aus. Schließlich ist jeder schon einmal bei einer Serie hängen geblieben, deren letzte Folge eigentlich bereits drei Folgen zuvor die letzte sein sollte. Eine längere Aufzeichnung deiner Einschlaf- und Aufwachzeiten kann dagegen Rückschlüsse auf deinen Tagesrhythmus ermöglichen. Werden diese Daten mit anderen Informationen kombiniert, entstehen zusätzliche Interpretationsmöglichkeiten.

Nicht alle derartigen Schlussfolgerungen müssen richtig sein. Eine Anwendung kann fehlende Bewegung fälschlicherweise als Schlaf interpretieren oder die Aktivität eines Geräts mit der Aktivität seines Besitzers verwechseln. Daten aus Verbrauchergeräten sind häufig Näherungswerte und keine medizinischen Messungen. Das ändert jedoch nichts daran, dass selbst unvollkommene Informationen verwendet werden können, um ein Nutzerprofil zu erstellen.

Besondere Aufmerksamkeit verdienen Daten über Symptome, Medikamente, psychische Gesundheit, Fruchtbarkeit oder chronische Erkrankungen. Anders als die Ergebnisse eines Spaziergangs betreffen sie Angelegenheiten, die viele Menschen ausschließlich ihrem Arzt oder nahestehenden Personen anvertrauen. Ihre Offenlegung kann unangenehm sein und unter bestimmten Umständen auch ernstere Folgen haben. Deshalb sollten wir mit solchen Informationen vorsichtiger umgehen als mit gewöhnlichen Einstellungen zur Darstellung einer Anwendung.

Wichtig ist außerdem, dass Gesundheitsinformationen nicht immer unter einer offensichtlich erkennbaren Bezeichnung auftreten. Manchmal bestehen sie aus Notizen, Antworten in einem Fragebogen, dem Suchverlauf oder Informationen, die aus dem Verhalten des Nutzers abgeleitet werden. Ein Programm muss nicht ausdrücklich nach einer bestimmten gesundheitlichen Beschwerde fragen, um trotzdem Daten zu verarbeiten, die Hinweise darauf liefern.

Was bedeutet Synchronisierung eigentlich?

Das Wort „Synchronisierung“ klingt beruhigend. Es erinnert an Ordnung, Übereinstimmung und Geräte, die wie ein außergewöhnlich diszipliniertes Team zusammenarbeiten. In der Praxis bedeutet es, dass Informationen zwischen bestimmten Geräten oder Diensten übertragen oder miteinander abgeglichen werden. Wie genau das geschieht, hängt von der jeweiligen technischen Lösung ab.

Nehmen wir an, du trägst dein Körpergewicht in eine Anwendung auf deinem Smartphone ein. Wenn die Daten ausschließlich lokal gespeichert werden, kannst du sie zusammen mit dem Gerät verlieren, sofern du keine Sicherungskopie angelegt hast. Aktivierst du dagegen die Synchronisierung mit einem Onlinekonto, kann es wesentlich einfacher werden, deine Aufzeichnungen auf einem neuen Smartphone wiederherzustellen. Das ist ein echter Vorteil, besonders bei Informationen, die über viele Monate gesammelt wurden.

Gleichzeitig kann Synchronisierung bedeuten, dass Daten das Gerät verlassen. Deshalb lohnt es sich herauszufinden, wer den Dienst betreibt, welche Informationen übertragen werden, wie lange sie gespeichert bleiben und ob du sie löschen kannst. Der Begriff „Cloud“ beantwortet diese

Fragen nicht. Schließlich ist die Cloud keine geheimnisvolle atmosphärische Substanz, die Daten speichert, ohne dass irgendjemand Verantwortung dafür übernehmen müsste. Es handelt sich um eine IT-Infrastruktur, die von konkreten Unternehmen oder anderen Organisationen betrieben wird.

Manche Dienste ermöglichen es, die Synchronisierung einzelner Datenkategorien getrennt zu steuern. Andere bieten lediglich die Möglichkeit, die gesamte Funktion ein- oder auszuschalten. Es kommt auch vor, dass bestimmte Informationen für die Nutzung eines Dienstes unverzichtbar sind, während zusätzliche Angaben freiwillig bleiben. Bevor du Einstellungen veränderst, solltest du deshalb nicht nur den möglichen Vorteil für deine Privatsphäre berücksichtigen, sondern auch die Folgen für die Funktionsweise der Anwendung.

Eine praktische Übung erfordert keinerlei Spezialwissen. Öffne eine Gesundheits-App, die du tatsächlich verwendest, und suche nach den Einstellungen für Benutzerkonto, Synchronisierung oder Datensicherung. Überprüfe, ob du die auf deinem Konto gespeicherten Daten einsehen kannst und ob der Hersteller erklärt, nach welchen Regeln diese Informationen gespeichert werden. Du musst zunächst überhaupt nichts deaktivieren. Das erste Ziel besteht darin herauszufinden, für welches Funktionsmodell du dich entschieden hast, möglicherweise völlig unbewusst während der ersten Einrichtung.

Wenn du die Anwendung zur Überwachung wichtiger medizinischer Informationen verwendest, solltest du vor dem Abschalten der Synchronisierung sicherstellen, dass du weder benötigte Aufzeichnungen noch Funktionen zur Weitergabe von Daten an Personen verlierst, die an deiner medizinischen Versorgung beteiligt sind. Der Schutz der

Privatsphäre bedeutet nicht, wichtige Informationen ohne einen Plan zu ihrer Aufbewahrung zu beseitigen.

Wer kann auf deine Informationen zugreifen?

An dieser Stelle könnte man versucht sein, sich einen riesigen Saal vorzustellen, in dem Hunderte Mitarbeiter unsere Schlafdiagramme beobachten und über den gestrigen Bewegungsmangel diskutieren. Keine Sorge. So muss die Datenverarbeitung keineswegs aussehen. Viele Vorgänge können vollständig automatisiert ablaufen, während der menschliche Zugriff durch entsprechende Verfahren eingeschränkt wird. Wichtiger als die Vorstellung neugieriger Mitarbeiter ist deshalb die Frage, welche Unternehmen oder Organisationen an der Verarbeitung deiner Informationen beteiligt sind und welche Zwecke sie dabei verfolgen.

Die erste beteiligte Stelle ist normalerweise der Anbieter der Anwendung. Er benötigt möglicherweise bestimmte Daten, um dein Benutzerkonto zu verwalten, die Synchronisierung bereitzustellen oder die gewünschte Dienstleistung zu erbringen. Hinzu kommen Anbieter technischer Infrastruktur, analytischer Werkzeuge, technischer Unterstützung oder anderer Funktionen. Ihre Beteiligung bedeutet nicht automatisch, dass Daten verkauft oder unberechtigt verwendet werden. Entscheidend sind der Umfang der Verarbeitung, die jeweiligen Rollen der Unternehmen und die eingesetzten Schutzmaßnahmen.

Besonders hilfreich ist es, drei Situationen voneinander zu unterscheiden: die Übermittlung von Informationen an ein Unternehmen, das im Auftrag des Anbieters arbeitet, die Weitergabe von Daten an eine andere Stelle für deren eigene Zwecke und die Veröffentlichung von Informationen durch den Nutzer selbst. Jede dieser Situationen hat andere

Konsequenzen. Im ersten Fall kann ein externes Unternehmen bestimmte technische Aufgaben übernehmen. Im zweiten wird wichtig, warum und auf welcher Grundlage der Empfänger die Daten verwendet. Im dritten kann die Entscheidung bei dir liegen, beispielsweise wenn du deine sportlichen Leistungen veröffentlichst.

Gerade dieser letzte Fall überrascht viele Menschen. Eine Sport-App fordert dich auf, deine Leistung zu teilen, also veröffentlichst du die Karte deines morgendlichen Laufs. Eine wunderschöne Strecke, ein beeindruckendes Tempo und eine sorgfältig ausgewählte Bildunterschrift. Das Problem besteht darin, dass die Karte möglicherweise den Start- und Endpunkt deines Trainings zeigt. Wenn du regelmäßig direkt vor deiner Haustür losläufst, kann dein öffentliches Profil mehr über dich verraten, als du beabsichtigt hast.

Deshalb musst du keineswegs auf das Teilen deiner Erfolge verzichten. Es lohnt sich jedoch, die Sichtbarkeitseinstellungen deines Profils, deiner Strecken und einzelner Aktivitäten zu überprüfen. Falls die Anwendung das Ausblenden bestimmter Streckenabschnitte ermöglicht, kannst du diese Funktion in Betracht ziehen. Dabei solltest du bedenken, dass ihre Wirksamkeit von der konkreten technischen Umsetzung abhängt. Eine andere Möglichkeit besteht darin, ausschließlich das Ergebnis zu veröffentlichen, ohne eine detaillierte Karte hinzuzufügen.

Privatsphäre beginnt damit, die eigenen Anwendungen zu kennen

Das größte Problem vieler Nutzer ist nicht eine einzelne riskante Entscheidung, sondern die fehlende Übersicht darüber, wie vielen Diensten sie bereits Informationen anvertraut haben. Eine App fürs Training, eine zweite für die

Ernährung, eine dritte für den Schlaf und eine vierte zur Überwachung bestimmter Körperwerte. Die fünfte wurde während eines Neujahrsschubs voller Motivation installiert und dient seitdem als digitales Erinnerungsstück an ehrgeizige Vorsätze.

Jeder dieser Dienste kann über ein eigenes Benutzerkonto, eine eigene Datenhistorie und eigene Einstellungen verfügen. Manche sind mit einer systemweiten Gesundheitsplattform verbunden, andere mit einem Gerät am Handgelenk und wieder andere mit einem sozialen Netzwerk. So entsteht ein Geflecht von Verbindungen, das sich anhand eines einzigen Bildschirms kaum beurteilen lässt.

Ein guter Anfang besteht darin, eine einfache Übersicht anzulegen. Du brauchst dafür weder eine Tabelle mit vierzehn Arbeitsblättern noch eine Präsentation für den Vorstand deines eigenen Körpers. Ein Blatt Papier oder eine gewöhnliche Notiz genügt. Darauf schreibst du die Namen der Gesundheits-Apps, die du aktiv verwendest. Notiere bei jeder Anwendung, wofür sie gedacht ist, ob sie ein Benutzerkonto benötigt und ob sie Informationen speichert, die du als besonders privat betrachtest.

Anschließend solltest du dir die Programme ansehen, die du nicht mehr verwendest. Nur weil eine Anwendung nicht mehr auf deinem Bildschirm erscheint, bedeutet das nicht unbedingt, dass die Verarbeitung der auf ihren Servern gespeicherten Daten beendet wurde. Das Entfernen eines App-Symbols und das Löschen eines Benutzerkontos sind häufig zwei unterschiedliche Vorgänge. Ebenso wenig solltest du annehmen, dass jedes Benutzerkonto eine umfangreiche medizinische Historie enthält. Zunächst gilt es

festzustellen, welche Informationen tatsächlich gespeichert wurden.

Bei dieser Überprüfung stellst du vielleicht fest, dass manche Anwendungen dieselben Aufgaben erfüllen. Zwei Programme zählen deine Schritte, drei zeichnen deine Aktivitäten auf, und ein viertes erinnert dich daran, dich mehr zu bewegen, obwohl die drei anderen ihm gerade mitgeteilt haben, dass du einen Spaziergang beendet hast. Wenn du die Zahl ähnlicher Dienste reduzierst, kann das die Verwaltung deiner Daten vereinfachen, die Anzahl deiner Benutzerkonten verringern und die Kontrolle über deine Einstellungen erleichtern.

Das bedeutet nicht automatisch, dass eine einzelne Anwendung immer sicherer wäre als mehrere. Entscheidend sind ihre tatsächlichen Praktiken und der Umfang der gesammelten Informationen. Weniger unnötige Dienste bedeuten jedoch normalerweise auch weniger Stellen, deren Einstellungen regelmäßig überprüft werden müssen.

Die erste Entscheidung, die wirklich etwas verändert

Angenommen, du entdeckst eine Anwendung, die du zuletzt vor zwei Jahren verwendet hast. Damals hast du darin ein Ernährungstagebuch geführt, dein Gewicht dokumentiert und ein Onlinekonto genutzt. Heute benötigst du diese Funktionen nicht mehr. Was solltest du tun?

Überprüfe zunächst, ob du dich noch bei deinem Benutzerkonto anmelden und die verfügbaren Informationen einsehen kannst. Falls die Aufzeichnungen für dich nützlich sind, suche nach einer Möglichkeit, sie zu exportieren. Anschließend informierst du dich darüber, wie du dein Benutzerkonto oder deine Daten löschen kannst. Manche Dienste ermöglichen es, diesen Vorgang selbstständig

einzuleiten, bei anderen musst du dich an den Anbieter wenden. Bedenke dabei, dass die Löschung nicht unbedingt sofort sämtliche Kopien umfasst, beispielsweise Informationen, die aus berechtigten rechtlichen Gründen noch für einen bestimmten Zeitraum aufbewahrt werden.

Wichtig ist die Reihenfolge. Wenn du zuerst die Anwendung entfernst und dabei den Zugang zu deinen Anmeldedaten verlierst, kann es später schwieriger werden, dein Benutzerkonto aufzuräumen. Das ist kein unlösbares Problem, aber zusätzliche Arbeit, die sich normalerweise vermeiden lässt.

Wenn die Anwendung dagegen weiterhin nützlich ist, musst du sie nicht löschen. Überprüfe stattdessen, ob du den Umfang der Informationen einschränken kannst, die du dort eingibst. Vielleicht genügen für dein Ziel grundlegende Messwerte, während ausführliche medizinische Notizen überhaupt nicht erforderlich sind. Eine bewusste Entscheidung sollte sich danach richten, welche Funktion du tatsächlich nutzen möchtest.

Denke außerdem daran, dass manche Daten für die Kontinuität deiner medizinischen Versorgung wichtig sein können. Wenn eine Anwendung Teil einer empfohlenen Überwachung ist oder dazu dient, medizinischem Personal Ergebnisse zu übermitteln, solltest du Veränderungen bei ihrer Nutzung mit der zuständigen Fachperson abstimmen.

Die wichtigste Erkenntnis dieses Kapitels ist einfach: Gesundheitsinformationen bilden keine einzige, in sich geschlossene Einheit. Sie entstehen an unterschiedlichen Stellen, werden zwischen Diensten übertragen und können für unterschiedliche Zwecke verwendet werden. Solange du nicht weißt, welche Werkzeuge du nutzt und wo deine Daten

gespeichert werden, fällt es schwer, bewusste Entscheidungen zu treffen.

Du musst nicht sofort die gesamte digitale Infrastruktur verstehen. Es reicht, wenn du aufhörst, deine persönlichen Informationen als unsichtbares Anhängsel bunter Diagramme zu betrachten.

Dein Smartphone darf deine Schlafhistorie kennen. Du hast allerdings jedes Recht zu erfahren, wer diese Historie speichert und unter welchen Bedingungen. Selbst wenn das Diagramm vor allem darauf hindeutet, dass du abends früher ins Bett gehen solltest.

Kapitel 2 - Kostenlose App, äußerst persönliche Währung

Auf dem Bildschirm deines Smartphones erscheint eine Werbung: „Lerne deinen Körper besser kennen. Umfassende Gesundheitsanalyse völlig kostenlos!“ Das Angebot klingt verlockend. Du musst lediglich die Anwendung installieren, ein Benutzerkonto erstellen, einige Fragen beantworten und kannst anschließend Funktionen nutzen, die vor nicht allzu langer Zeit ausschließlich teuren Geräten vorbehalten zu sein schienen.

Der erste Fragebogen erkundigt sich nach deinem Alter. Der zweite nach deinem Körpergewicht. Der dritte nach deinem Aktivitätsniveau, Schlafproblemen und täglichen Wohlbefinden. Der vierte möchte deine Ziele kennenlernen. Der fünfte hat offenbar vor, dich besser kennenzulernen als die meisten deiner entfernten Verwandten. Nach wenigen Minuten hast du das Gefühl, dass die Anwendung deine Biografie schreiben könnte, obwohl sie dir noch immer kein einziges brauchbares Diagramm gezeigt hat.

Bedeutet das, dass gerade jemand versucht, dir persönliche Daten abzuluchsen? Nicht unbedingt. Manche Fragen können für die Funktionsweise des Programms durchaus gerechtfertigt sein. Eine Anwendung, die bestimmte Körperwerte analysiert, benötigt möglicherweise Informationen, die für ihre Berechnungen notwendig sind. Ein Gesundheitstagebuch muss es ermöglichen, Beobachtungen festzuhalten. Ein Programm zur Trainingsplanung kann Angaben über die körperliche Aktivität und die Ziele des Nutzers verwenden.

Das eigentliche Problem liegt woanders. Wir nehmen leicht an, dass sämtliche verlangten Informationen ein natürlicher Preis für die Nutzung eines kostenlosen Dienstes sind. Dabei lohnt es sich, zwischen tatsächlich notwendigen Daten und zusätzlichen Angaben zu unterscheiden, deren Weitergabe anderen Zwecken dienen oder lediglich das Nutzerprofil erweitern kann.

Eine kostenlose Anwendung muss ihr Geld nicht mit deinen Daten verdienen. Sie kann durch kostenpflichtige Zusatzfunktionen, Abonnements, den Verkauf von Geräten, institutionelle Unterstützung oder andere Einnahmequellen finanziert werden. Manche Dienste nutzen Informationen ihrer Nutzer allerdings für Analysen, die Personalisierung von Werbung oder die Weiterentwicklung ihrer Produkte. Das Geschäftsmodell ist deshalb wichtig, weil es beeinflusst, welche Daten ein Unternehmen sammeln möchte.

Und genau deshalb ist die Diskussion über die tatsächlichen Kosten nicht beendet, nur weil auf dem Preisschild null Złoty stehen.

Warum möchte die Anwendung so viel über dich wissen?

Stell dir vor, du bestellst in einem Café einen Tee. Der Verkäufer fragt dich nach der Größe des Bechers, der Teesorte und ob du vielleicht eine Scheibe Zitrone möchtest. Alles vollkommen verständlich. Anschließend interessiert er sich für deine Schlafenszeiten, deine Allergiegeschichte und dein Stressniveau während der vergangenen sechs Wochen. Vielleicht bereitet er gerade den am stärksten personalisierten Tee in der Geschichte der Gastronomie zu. Trotzdem darfst du fragen, ob all diese Informationen wirklich notwendig sind.

Genauso solltest du die Formulare in Gesundheits-Apps betrachten. Jede Frage sollte im Zusammenhang mit der angebotenen Funktion einen nachvollziehbaren Sinn ergeben. Wenn ein Programm deinen Energiebedarf anhand eines bestimmten Berechnungsmodells ermittelt, benötigt es möglicherweise bestimmte Angaben über dich. Wenn es dagegen lediglich die Anzahl getrunkener Wassergläser dokumentiert, ist der Umfang der notwendigen Daten normalerweise wesentlich geringer.

Wichtig ist außerdem die Unterscheidung zwischen Grundfunktionen und zusätzlichen Angeboten. Eine Anwendung kann möglicherweise ohne ein detailliertes Nutzerprofil funktionieren, aber nach Eingabe weiterer Informationen umfangreichere Analysen anbieten. In diesem Fall solltest du überlegen, ob der zusätzliche Nutzen wirklich groß genug ist, um die Weitergabe der entsprechenden Daten zu rechtfertigen.

Manche Formulare enthalten Felder, die als Pflichtangaben gekennzeichnet sind, obwohl ihre Bedeutung nicht offensichtlich ist. Allein diese Kennzeichnung beweist noch nicht, dass die Anforderung gerechtfertigt ist. Du kannst die Erklärungen des Herstellers überprüfen, nach einer Möglichkeit suchen, den entsprechenden Schritt zu überspringen, oder ein anderes Werkzeug auswählen, das weniger Informationen verlangt.

Ebenso wichtig ist es, Daten nicht vorsorglich einzugeben. Wenn eine Anwendung ein Feld für zusätzliche medizinische Notizen bereitstellt, musst du dort nicht deine gesamte Behandlungsgeschichte eintragen, nur weil ausreichend Platz dafür vorgesehen wurde. Die Benutzeroberfläche mag dich zur Vollständigkeit ermuntern, dein Ziel sollte jedoch darin bestehen, die Informationen