LIEWO
SONNTAGSZEITUNG
Für Liechtenstein und das obere St. Galler Rheintal
www.liewo.li
15. März 2020 | Nr. 10

Wetter › 57

15°

SMARTPHONE
Der Datenschutz wird bei Apps oft vergessen
Thema 13

OBSTBÄUME
In Schellenberg wachsen seltene Baumsorten
Interview 20

LEICHTATHLETIN
Ihre Krankheit zwingt Eva Ulmann zum Aufhören
Sport 62

Varghese Georg Thaniyath

Er schenkt ein Dach überm Kopf

Thema

Wie man persönliche Daten besser schützt

Fünf Tipps, die relativ wenig Aufwand beanspruchen, helfen bereits weiter.

Seite 16

Dass Apps die Informationen ihrer Nutzer horten und weitergeben, ist durchaus bekannt. Studien belegen ein geringes Vertrauen. Sobald man das Smartphone in den Händen hält, rückt der Datenschutz trotzdem oft in den Hintergrund.

Seite 14

Der Spion auf dem eigenen Smartphone

Foto: iStock

Studie

«Out of Control»

Mitte Januar gab die norwegische Verbraucherschutzorganisation NCC eine Studie in Auftrag, bei der die Cybersecurity-Firma Mnemonic zehn beliebte Anwendungen des Google Play Stores daraufhin untersuchte, welche Daten sie an Drittanbieter weiterleiten. Privatsphäre gegen App lautet das Tauschgeschäft, welches gemäss dem Titel der Untersuchung «Out of Control» geraten sei. Die Zahlen sprechen für sich: 88 000 Web-Anfragen von 216 verschiedenen Domains wurden über die Apps registriert. In den Werbebereichen fanden sich mindestens 135 Unternehmen. Die GPS-Standorte, die Religion sowie sexuelle Orientierung ihrer Nutzer stellen alle zehn Apps als wesentlichen Bestandteil ihres Geschäftsmodells zur Verfügung – besonders die Dating-App «Grindr» für schwule, bisexuelle und transsexuelle Männer sende viele Informationen an Drittthersteller.

Die Studie weist darauf hin, dass die App-Hersteller das Sammeln und Weitergeben der Daten als fixe Einnahmen in ihr Geschäftsmodell einrechnen. An ihre Informationen gelangen Drittthersteller oft über Software-Development-Kits (SDK), wie sie unter anderem für Kreditkartenzahlungen existieren. Hersteller übernehmen diese Codes für ihre App, um sich auf diese Weise das Programmieren solcher standardisierten Funktionen zu ersparen. «Informationen in den Datenschutzbestimmungen können den Nutzer nicht völlig auf die Konsequenzen aufmerksam machen, die mit dem Teilen von persönlichen Daten an Drittstellen einhergeht», lautet das Fazit der Studienautoren. Ein weiterer Kritikpunkt lautet, dass Einstellungen zugunsten der Privatsphäre tief in den Einstellungen versteckt sind. *(gk)*

Privatsphäre war gestern

Die **Nutzung von Apps** wie Whatsapp, Facebook und diversen Spielen ist nur auf den ersten Blick gratis. Statt mit Geld wird mit persönlichen Informationen bezahlt.

Gary Kaufmann
gkaufmann@medienhaus.li

Als George Orwell vier Jahre nach dem zweiten Weltkrieg im Roman «1984» einen totalitären Überwachungsstaat vorstellte, schien dieser weit entfernt zu sein. Der darin propagierte Slogan «Big Brother is watching you» könnte mit dem Aufkommen von Gesichtserkennungs-Apps kaum aktueller sein. Im Alltag ist die Datengier bereits omnipräsent. Nach einem Kaffee im Restaurant bittet das Smartphone um eine Bewertung des Lokals. Bucht man ein Flugticket, ist die Werbung für ein Hotel in der Zieldestination nicht weit entfernt.

Was Fiktion und Realität voneinander unterscheidet: Überhaupt ermöglicht wird dies alles durch eine undurchsichtige Weitergabe von persönlichen Daten, die ein Grossteil der Gesellschaft online über sich und andere mehr oder weniger freiwillig preisgibt – im Gegenzug für die Nutzung von Apps. Marie-Louise Gächter, Leiterin der Datenschutzstelle Liechtenstein, appelliert neben den Unternehmen, die Informationen ihrer Nutzer in das Geschäftsmodell einkalkulieren, genauso an die Eigenverantwortung der Bürger. «Immer mehr Leute sind gut informiert. Es geht vielmehr um ein Abwägen zwischen Komfort und dem Stellenwert der Privatsphäre», meint sie. In Liechtenstein klickt gemäss einer Umfrage des Liechtenstein-Instituts knapp die Hälfte sofort weg, sobald Apps sie mit einer Datenschutzerklärung konfrontieren.

Puzzlestück für Puzzlestück

Das Problem ist weniger einer mangelhaften Aufklärung geschuldet, sondern die Nutzer scheuen sich vor dem zeitlichen Aufwand, der mit den Sicherheitsmassnahmen einhergeht. Und selbst diese können keine 100-prozentige Sicherheit gewährleisten, betont Marie-Louise Gächter. Aus den wenigen Beschwerden, die bisher aufgrund von Apps eingegangen sind, leitet sie ab, dass der Datenschutz häufig ausgeblendet wird, sobald das Smartphone in der Hand liegt. Ihr Stellvertreter Michael Valersi kennt die Ursache dafür: «In der realen Welt hat unser Handeln direkt spürbare Konsequenzen. Wenn wir digital unterwegs sind, sind diese hingegen weniger greifbar.»

> Knapp die Hälfte klickt weg, sobald sie mit dem Datenschutz konfrontiert wird.

Ein vor wenigen Wochen in der «New York Times» veröffentlichter Bericht zeigt auf, welche Konsequenzen für die Nutzung von Apps in Kauf genommen werden. Dieser berichtet über eine Gesichtserkennungs-Technologie des US-Unternehmens Clearview, die bereits mehrere Millionen Personen identifiziert. Zusätzlich spuckt sie ihre sexuelle Orientierung, Religion und weitere persönliche Informationen aus. Zu

Foto: Roland Rick

Auf dem Smartphone wird der Datenschutz oft ausgblendet, finden Michael Valersi und Marie-Louise Gächter von der Datenschutzstelle Liechtenstein.

Foto: iStock

Rund zwei Drittel der Liechtensteiner sind gemäss einer Umfrage täglich auf sozialen Plattformen unterwegs, obwohl sie sich dabei nicht sicher fühlen.

den rund 600 Kunden gehören sowohl nordamerikanische Behörden als auch Privatunternehmen, wobei der Betreiber keine Namen preisgibt. Die Datenschutzstelle Liechtenstein habe bislang noch keine Anfragen oder Beschwerden bezüglich dieser App erhalten.

Die Flutwellen an Bildmaterial (über drei Millionen Fotos), welche die Gesichtserkennungs-App benötigt, stammen aus sozialen Netzwerken wie Facebook und Instagram. Zusammengesetzt ergeben die vermeintlich harmlosen Daten ein umfassendes Informationsgeflecht – Michael Valersi verwendet an Vorträgen und Workshops häufig eine Puzzle-Metapher dafür. «Die Daten werden umso wertvoller, je mehr Querverbindungen zu Daten aus anderen Quellen hergestellt werden können», hält er fest. Vor allem Standortdaten seien kostbar, ergänzt Gächter. Bei einer gewissen Regelmässigkeit würden sie viel über einen aussagen. Als Beispiel nimmt sie einen Nutzer, der gemäss GPS dreimal in der Woche denselben Fussballplatz aufsucht. Im Kontext mit einer Gesundheits-App und weiteren Anwendungen entsteht schnell das Bild eines leidenschaftlichen Sportlers. Die Folge davon ist Werbung, die auf sein persönliches Profil zugeschnitten ist. Und gerade diese Art der Produktplatzierung reizt die Unternehmen. «Ein Luxusautohersteller hat kein Interesse daran, jemandem seine Autos anzupreisen, der sich nicht einmal einen Kleinwagen leisten kann», erklärt die Leiterin der Datenschutzstelle.

Eine US-App erkennt mehrere Millionen Leute am Gesicht.

Kein Vertrauen in Facebook

Es ist ein offenes Geheimnis, dass sich Gratis-Apps durch Werbung respektive den Verkauf der gesammelten Daten finanzieren. Dies ist den Nutzern durchaus bekannt, wie eine Umfrage des Liechtenstein-Instituts zum Thema Datenschutz bestätigt. In Auftrag gegeben wurde sie von der Datenschutzstelle. 4000 zufällig ausgewählten Liechtensteinern wurden die Fragebogen zugestellt, wovon fast ein Drittel diese ausfüllten. Die Ergebnisse sollen noch im März präsentiert werden, wie Marie-Louise Gächter klarstellt.

Nichtsdestotrotz könne die Datenschutzstelle bereits heute erste Beobachtungen verraten. So würden rund zwei Drittel der liechtensteinischen Bevölkerung die sozialen Medien nutzen; die meisten davon täglich. Allerdings vertrauen die wenigsten den Plattformen, was den Umgang mit ihren persönlichen Daten betrifft. «Die überwiegende Mehrheit der Liechtensteiner hält den Schutz ihrer persönlichen Daten für sehr wichtig und ist überzeugt, dass die vor kurzem erfolgte Stärkung der Datenschutzbestimmungen hierzulande richtig war», fasst Marie-Louise Gächter zusammen. Und das, obwohl in der Regel vorderhand vor allem der bürokratische Aufwand gesehen werde.

Schutz der persönlichen Daten wird als wichtig erachtet.

Jeder muss selbst entscheiden

Die Datenschutzstelle Liechtenstein beschäftige sich nicht explizit mit einzelnen Applikationen. Da deren Hersteller beinahe in allen Fällen ihren Sitz im Ausland haben, könnte sie Beschwerden meistens lediglich an die zuständige Behörde vor Ort weiterleiten. Stattdessen konzentriert man sich hierzulande auf eine «technikneutrale» Beratung. Soll heissen, dass die Datenschutzstelle etwa Beratungen anbietet, Infoveranstaltungen durchführt, allgemein für das Thema sensibilisiert und auf die Gefahren im Internet hinweist. Letztlich müsse jedoch jeder für sich selbst entscheiden, wie er mit seinem Smartphone sowie anderen Endgeräten umgehen möchte. «Die Entscheidung, eine bestimmte Applikation zu verwenden oder nicht, dürfen und wollen wir dem Bürger nicht abnehmen», sagt Marie-Louise Gächter.

Kommentar

Gary Kaufmann
gkaufmann@medienhaus.li

Bitte noch mehr Transparenz

Google weiss nicht nur, was ich letzten Sommer getan habe – seit ich ein Android-Smartphone besitze, folgt mir der Datensammler auf Schritt und Tritt. Um mich an meine Reisen in den vergangenen Jahren zu erinnern, brauche ich bloss den US-Konzern zu fragen.

Innerhalb von wenigen Klicks stellen mir Apps sämtliche Daten, die sie von mir horten, als Paket zur Verfügung. Abgesehen von einem Schwelgen in Erinnerungen hält sich der Nutzen davon in Grenzen. Jeder weiss selbst am besten, was er im World Wide Web anstellt. Statt Transparenz sorgt das weite Nebenmeer an Daten, die eine solche Abfrage offenbart, für Paranoia. Insbesondere, weil der Durchschnittsnutzer mit kryptischen HTML-Dateien sowie anderen Formaten wenig anzufangen weiss. Ein Blick in die Datenschutzbestimmungen einer App bietet zwar langwierige Texte und Hyperlinks, doch die langersehnte Erleuchtung bleibt meistens aus.

Das Problem besteht nicht darin, dass Apps sich vernetzen und so unsere Informationen zusammenschustern. Hierbei handelt es sich um die bekannte «Währung», mit der wir ihre unentgeltlichen Dienstleistungen bezahlen. Viel interessanter wäre, an wen Google und Co. die von ihren Nutzern aufgesaugten Daten weitergeben. Um an eine Liste dieser Drittanbieter zu kommen, muss jeder Einzelne intensiv nachbohren, einen ziemlichen Aufwand betreiben.

5 Tipps für mehr Sicherheit im Netz

Eine vollständige Kontrolle über die eigenen Daten lässt sich im Internet nicht garantieren. Allerdings gibt es einige **Massnahmen mit überschaubarem Aufwand,** mit denen sich die persönlichen Informationen auf dem Smartphone besser schützen lassen. Die «Liewo» hat bei der Datenschutzstelle Liechtenstein nachgefragt. Text: Gary Kaufmann

Bei einer Veranstaltung am 30. Januar im Vaduzer Saal – anlässlich des Europäischen Datenschutztags – regte Marie-Louise Gächter mit einem Beispiel zum Nachdenken an. Sie entführte das Publikum in einen gewöhnlichen Donnerstagmorgen des Max Musters, der in einer knappen halben Stunde zehn Apps und Websites benutzte. Dabei schrieb er unter anderem Whatsapp-Nachrichten, rief seine E-Mails ab und kaufte sich ein Busticket. Während dieser kurzen Zeit hinterliess er online Spuren bei über 180 Drittanbietern. Mit den folgenden fünf Tipps lässt sich diese Zahl drastisch reduzieren:

Foto: iStock

Jede Zugriffsberechtigung einer App sollte hinterfragt werden.

1. Seriöse Quellen

«Zuerst sollte sich der Nutzer diese Fragen stellen: Brauche ich diese App wirklich, und warum möchte ich sie unbedingt ausprobieren?», empfiehlt Michael Valersi, stellvertretender Leiter der Datenschutzstelle. Aufmerksamkeit ist bereits vor dem Download geboten. Apps sollten nur von den offiziellen Vertriebsplattformen der Hersteller bezogen werden. Im Fall von Android ist dies «Google Play», das entsprechende Pendant auf iPhone heisst «App Store». Aber auch dort tummeln sich zahlreiche Betrugsprogramme, die sich – mit ähnlichen Namen und täuschend ähnlichen Logos – für etwas anderes ausgeben.

Ein Blick auf die Bewertungen und Kommentare bringt oft Licht ins Dunkle, welche Hersteller nur auf Abzocke aus sind. Genauso sollte man die Produkterklärungen lesen, so Michael Valersi: «Hinweise für Betrugs- und Schad-Apps sind etwa schlechte Bewertungen oder ein reisserischer Stil für die Bewerbung einer bestimmten, oft technisch nicht umsetzbaren Funktionalität oder auch rasche Gewinnaussichten.» Ebenfalls sollte berücksichtigt werden, wie die Urheber ihre Einnahmen generieren. Hinter vermeintlich kostenlosen Spielen können sich sogenannte In-App-Käufe verstecken. Bei einem ungutem Gefühl sollte man lieber nicht auf «Download» klicken.

2. Vorsichtig herantasten

Hat man eine App erst einmal für vertrauenswürdig befunden und auf dem Smartphone installiert, verhält es sich wie mit dem Fahrrad: Zuerst sollte man mit Stützrädern in die Pedale treten, bis man sich sicher fühlt. Michael Valersi gehe bei neuen Apps immer zurückhaltend vor, hinterfrage sämtliche Zugriffsberechtigungen auf Fotos, Videos und andere Daten. In einem nächsten Schritt werfe er einen genauen Blick auf die Einstellungen. «So macht die Einstellung ‹Standortabfragen erlauben› in den meisten Fällen wenig Sinn, wenn es sich um keine Navigationsanwendung handelt», argumentiert er. Oft können die Apps ihre Hauptfunktion trotzdem erfüllen, selbst wenn einige Zusatzfunktionen wegen den fehlenden Berechtigungen streiken. Der Fahrplan auf der SBB-App lässt sich auch abfragen, ohne dass man seinen Standort bekannt gibt. Bei aktiviertem GPS wird dafür automatisch die nächstgelegene Haltestelle angezeigt. Je nachdem, welchen Service man tatsächlich beansprucht, können Nutzer gewisse Anfragen getrost ablehnen.

3. Werbeblocker installieren

Was für das Surfen auf dem Computer gilt, sollte man sich auch für das Smartphone zu Herzen nehmen. Dementsprechend garantiert die Installation eines Werbeblockers mehr Sicherheit im World Wide Web. Auf Smartphones lassen sich nämlich genauso Anti-Tracking-Tools aktivieren. Häufig bieten Browser eine entsprechende Erweiterung an. Automatische Weiterleitungen von E-Mails und anderen Datenträgern sollten unterbunden werden, um die Übersicht zu behalten.

4. Bilanz ziehen

Man kennt es von den eigenen vier Wänden: Im Verlauf der Zeit sammeln sich zu Hause allerlei Staubfänger an. Dasselbe gilt sinngemäss auch für das Smartphone. Manche Apps werden einmalig für einen bestimmten Zweck gebraucht – zum Beispiel das ÖV-Angebot einer bestimmten Stadt während der Ferien – und haben dadurch einen festen Platz auf dem Gerät, womit sie ein weiterer Informant für Drittanbieter bleiben. «Nicht mehr verwendete Apps sollten regelmässig gelöscht werden», rät Michael Valersi. Nach einer bestimmten Probezeit sei zu prüfen, ob eine App die Anforderungen, wegen der man sie ursprünglich runtergeladen hat, überhaupt erfüllt. Nach Updates sollten immer die Einstellungen einer App kontrolliert werden, weil diese dadurch häufig auf den Standard zurückgestellt werden.

5. Aufräumen

Entscheidet man sich dazu, von einer bestimmten App Abschied zu nehmen, ist es mit dem Bestätigen der «Deinstallation» nicht getan. Gerade bei sozialen Netzwerken, aber auch bei anderen Angeboten sind bestimmte Nutzerprofile damit geknüpft, die vorher zu löschen sind. Ansonsten sind die persönlichen Informationen darauf für den Anbieter sowie Drittanbieter weiterhin verfügbar. «In allen anderen Bereichen ist es selbstverständlich, dass man hinter sich aufräumt. Nur in der digitalen Welt wird es häufig vergessen», meint Marie-Louise Gächter.