ÖAW

ZURÜCK

05.11.2019

DAS VIRTUELLE ICH

Digitale Identitäten sind eine Voraussetzung für zahlreiche Apps & Services und gewinnen auch als elektronische Ausweise an Bedeutung. Welche Trends in diesem Bereich auf uns zukommen und warum die Sicherheit nicht auf der Strecke bleiben darf, berichtete René Mayrhofer, Informatiker und ehemaliger Android Sicherheitschef, im Rahmen einer Akademievorlesung an der ÖAW.

© Antoine Beauvillain/Unsplash

Von der E-Banking-App über Web-Streamings bis hin zum elektronischen Führerschein: Ohne Log-Ins und eine elektronische Identifikation kommt man in der digitalisierten Welt vielfach nicht mehr weit. Der Vormarsch der digitalen Identität eröffnet dabei neue Fragen über die Möglichkeiten und Grenzen des virtuellen Ichs.

René Mayrhofer vom Institut für Netzwerke und Sicherheit der Johannes Kepler Universität (JKU) Linz kennt diese sehr genau: Als ehemaliger Android Sicherheitschef war der Informatiker bei Google für die Absicherung dieses weltweit verbreiteten Smartphone-Systems zuständig. Am 12. November 2019 skizzierte er an der Österreichischen Akademie der Wissenschaften (ÖAW) in der Reihe der Akademievorlesungen, welche Entwicklungen und Perspektiven in diesem Bereich zu beobachten sind.

Herr Mayrhofer, was ist eine digitale Identität?

René Mayrhofer: Darunter verstehen wir heute oft ein ganzes Sammelsurium von Log-In-Daten, die wir im Netz verwenden, vom E-Banking bis zu Social Media-Webseiten. Allgemeiner gesprochen sind digitale Identitäten aber Mengen von Attributen, die Eigenschaften natürlicher Personen beschreiben, wie zum Beispiel Namen, Alter, Wohnort und so weiter.

Wie weit ist die Digitalisierung der Identität schon vorangeschritten?

Mayrhofer: Derzeit werden ganz verschiedene Attribute einer Identität von Plastik- oder Papierdokumenten auf das Smartphone verschoben, von Führerscheinen über E-Cards bis zu Reisepässen. Das erfordert, dass wir uns Gedanken darüber machen, wie solche sensiblen Informationen sicher auf unseren Geräten genutzt werden können. Wir arbeiten an der JKU etwa daran mit, einen internationalen Standard für elektronische Führerscheine zu entwickeln. Das ist aber nur der erste Schritt der Digitalisierung.

Wie geht die Entwicklung weiter?

Mayrhofer: Ich denke, dass wir in den nächsten zehn Jahren sehen werden, dass weitere Identifikationsapplikationen auf unseren Smartphones landen. Danach rechne ich damit, dass diese Systeme in die Cloud wandern werden. Vom Öffnen von Türen in Gebäuden bis zur Grenzkontrolle werden die erforderlichen persönlichen Informationen und Berechtigungen dann in Nutzerprofilen gespeichert werden, die nicht mehr auf ein spezifisches Gerät angewiesen sind.

Wie ein digitaler Schatten, der mir überall hin folgt und verschiedenste Türen öffnen kann?

Mayrhofer: Ja, dahin geht der Trend, aber das passiert nicht über Nacht. Wir wissen heute, wie wir diverse Ausweisdokumente und Nutzerkonten auf Smartphones bringen können, es wird aber trotzdem noch Jahre dauern, bis eine breite Bevölkerungsschicht von dieser Möglichkeit Gebrauch macht.

Was sind die Vorteile einer Cloud-Lösung?

Mayrhofer: Das wäre vor allem bequem. Der Fingerabdruck oder ander biometrische Merkmale könnten dann sämtliche Ausweise und Log-Ins ersetzen. Die Sicherheit wird auch erhöht, weil Identitäten nicht mehr durch den Diebstahl eines Smartphones kompromittiert werden können.

Wie sieht es mit den Schattenseiten aus?

Mayrhofer: Wenn wir eine zentrale Datenbank mit allen nötigen Informationen haben, ist das natürlich ein Problem für den Datenschutz und die Privatsphäre. In Indien und China kann man derzeit sehen, dass der Aufbau solcher Datensammlungen demokratiepolitisch bedenklich ist. Wir sehen als Wissenschaftler, wohin die Reise geht, aber wir kennen auch die Risken. Systeme wie sie in Indien und China entstehen, sind nicht kompatibel mit europäischen Werten.

Das heißt, es geht nicht nur um technische Fragen, sondern auch darum, wie viel Macht wir unseren politischen Verantwortlichen geben wollen.

Die Frage ist, wie viel Macht wir allen künftigen Machthabern geben wollen. Die Architektur von digitalen Identitäten bestimmt, wer Zugriff auf welche Informationen bekommt. Das gilt dann auch für die Zukunft und ist damit auf jeden Fall eine politische Frage.

Ist eine Lösung, die persönliche Daten schützt und zudem ausreichend sicher und bequem zu nutzen ist, überhaupt möglich?

Mayrhofer: Als Wissenschaftler muss ich sagen: Wir wissen es noch nicht. Es gibt dezentrale Architekturen, die Bequemlichkeit, Sicherheit und Privatsphäre unter einen Hut bringen könnten. Aber wir haben keine fertige Lösung, das müssten wir mit Partnern über einen längeren Zeitraum untersuchen.

Als Laie fragt man sich oft, warum Dinge digitalisiert werden, wenn die Risiken so hoch sind.

Mayrhofer: Als Privatperson muss ich sagen, dass ich nicht sicher bin, ob ich will, dass meine Identität in der Cloud landet. Als Wissenschaftler fürchte ich aber, dass derartige Systeme kommen werden, ob wir das wollen oder nicht. Den Kopf in den Sand zu stecken ist sicher keine Lösung. Also versuche ich lieber jetzt steuernd einzugreifen. Ob das klappt, liegt aber nicht in den Händen von uns Wissenschaftlern. Wir müssen jetzt eine gesellschaftliche Debatte darüber anstoßen, welche Lösung wir wollen.

Bei manchen Themen, etwa E-Voting, sind die Risken der Digitalisierung für die meisten Experten aber dann doch zu hoch.

Mayrhofer: Ich spiele jetzt mal des Teufels Advokaten. Es gibt Gründe für E-Voting. Parteien haben oft Probleme, Wahlhelfer zu finden, es wird eine Menge Papier verschwendet und der Aufwand ist enorm. Vielleicht wollen die Menschen in Zukunft auch mehr direkte Demokratie, auch hier gäbe es Vorteile. Am Ende ist das immer eine Abwägung zwischen Chancen und Risiken. Persönlich überzeugen mich E-Voting-Systeme in dieser Hinsicht derzeit nicht.

Es gibt also noch einiges zu tun. Wie sieht es mit dem Zwischenschritt zur Smartphone-Lösung aus?

Mayrhofer: Hier sind wir, denke ich, auf einem guten Weg, Systeme zu entwickeln, die Sicherheit, Privatsphäre und einfache Nutzung gewährleisten.

Ist ein mögliches Knacken heutiger Kryptografieverfahren durch künftige Quantencomputer ein Thema bei der Entwicklung digitale Identitäten?

Mayrhofer: Wir haben an der JKU ein neues Labor (das LIT Secure and Correct Systems Lab, Anm.), an dem neun Institute beteiligt sind. Dort wird unter anderem an der Entwicklung sicherer Quantenkryptografie gearbeitet. Ich vertraue darauf, dass Lösungen bereitstehen werden, wenn die Quantencomputer so weit sind.

AKADEMIEVORLESUNGEN

← ZURÜCK

SHARE

QUICKLINKS

NEWS →

EVENTS →

PRESSE →

INTERN →

KARRIERE & JOBS

→ Offene Stellen an der ÖAW

→ Informationen zum Datenschutz bei der Übermittlung von Bewerbungen

OPEN CALLS

→ Preise für junge Wissenschaftler/innen

→ Stipendien für junge Wissenschaftler/innen

WIR SIND DIE ÖAW

© Copyright OEAW