Authentifizierung durch Verhalten

Die Authentifizierung von Internet-NutzerInnen ist vor allem für Finanztransaktionen, Vertragsabschlüsse oder sichere Zugänge zu Online-Konten wichtig. Mittlerweile ist diese Authentifizierung auch durch die Analyse des Verhaltens von NutzerInnen möglich. Konkret geht es um die Art und Weise, wie z.B. getippt wird (typischer Tastaturanschlag) und wie Smartphone-NutzerInnen ihr Gerät während der Eingabe halten. Aus der unterschiedlichen Dauer und Geschwindigkeit eines Tastendrucks lässt sich über eine kurze Zeitspanne ein individuelles Profil erstellen. Die Verfügbarkeit dieser persönlichen Daten ist aufgrund der zahlreichen eingebauten Sensoren gegeben. Die Authentifizierung mittels NutzerInnen-Verhalten läuft oft im Hintergrund herkömmlicher Login-Varianten und wird von Banken bereits kommerziell genutzt[45]. Neben Finanzdienstleistern sind Universitäten, E-Learning-Provider, Anwaltskanzleien, Online-Services und viele weitere Branchen Zielgruppe der Technologie.

Bisher wurden dafür individuelle Passwörter genutzt, die je nach gewählter Länge und Komplexität sicher oder unsicher sind. Auch Multifaktor-Logins anhand von Hardware-Tokens, Bankkarten oder Schlüssel in Kombination mit Einmalkennwörtern, PINs oder TANs sind übliche Authentifizierungsvarianten. Biometrische Merkmale werden immer öfter für die eindeutige Erkennung von Internet-NutzerInnen herangezogen. Dazu zählen Fingerabdrücke, Muster der Regenbogenhaut (Iris-Erkennung), Gesichtserkennung (siehe Thema „Gesichtserkennung“, S. 59) oder Stimmprofile. Diese bisherigen Authentifizierungsmethoden sind durch bewusste und durch die Individuen steuerbare Handlungen bestimmt. Die Analyse des NutzerInnenverhaltens kann dagegen im Hintergrund geschehen.

Nicht nur private Unternehmen haben Interesse an der neuen Authentifizierungs-Technologie, sondern auch die Forschungsbehörde des US-amerikanischen Militärs (DARPA) finanziert die Entwicklung von verhaltensanalytischen Technologien[46]. Gerade in diesem Kontext drängt sich die Frage auf, wie persönliche Daten, die durch Verhaltensauthentifizierung gesammelt werden, weiterverarbeitet werden (siehe Thema „Authentifizierung durch Verhalten“, S. 57). Mit dem Argument der Cybersicherheit könnten Staaten die Technologie nutzen, die andere Prinzipien anlegen, als es im europäischen Rechtsrahmen vereinbart ist. Auch Werbetreibenden stünden Daten zur Verfügung, die ohne Wissen und Zustimmung der KundInnen gesammelt werden können und mit denen diese durch das gesamte Internet verfolgt werden könnten.

Obwohl bereits Software existiert[47], die auf die Verschleierung von Verhaltensdaten abzielt (indem Eingaben um einige Millisekunden verzögert

[45] behaviosec.com/danske-bank-deploys-behaviosec/.

[46] opencatalog.darpa.mil/AA.html.

[47] chrome.google.com/webstore/detail/keyboard-privacy/aoeboeflhhnobfjkafamelopfeojdohk.

oder beschleunigt werden), bleibt die Frage der transparenten Anwendung von Verhaltensanalysetools offen. Hier könnte das österreichische Parlament mit gesellschaftlich verhandelten Transparenzrichtlinien bei der Generierung und Verarbeitung von verhaltensbezogenen Daten gestalterisch auf die Zukunft einwirken.

(DW)