piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Sehr geehrte Herr Bundesrat Berset

Sehr geehrte Damen und Herren

Vernehmlassungsantwort zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (Systematische Verwendung der AHV-Nummer durch Behörden)

Obschon sich die Piratenpartei bekanntlich bei allen Gesetzen bezüglich Datenschutz immer stark engagiert, wurden wir zur dieser Vernehmlassung leider nicht eingeladen. Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 7. November 2018 nehmen wir dennoch gerne Stellung und würden es zukünftig sehr begrüssen, wenn wir in ihre Adressatenliste aufgenommen werden.

Noch ein Hinweis: Wir finden es sehr bedenklich, dass Sie für die Stellungnahme auch ein proprietäres Dateiformat verlangen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Formate gibt. Dennoch entsprechen wir Ihrem Wunsch.

Grundlegendes

Die systematische Verwendung der AHVN13 (dreizehnstellige AHV-Nummer) als Identifikator im Rahmen aller möglichen behördlichen Aufgaben sehen wir als sehr grosse Gefahr. Sie wird von der Piratenpartei Schweiz NICHT unterstützt. Alle entsprechenden Gesetzesanpassungen sind somit explizit zu streichen.

Gerne wiederholen wir einige Grundlagen aus Ihrem Bericht: Die AHV-Nummer (AHVN) ist ein 13-stelliger, nicht sprechender Personenidentifikator. Darüber hinaus enthält die AHVN keine Informationen über den jeweiligen Inhaber, sie erlaubt also keine Rückschlüsse auf dessen persönliche Eigenschaften.

Diese Nummer ist eindeutig und einmalig für alle in der Schweiz wohnhaften Personen und solche, die irgendwann ein Beitrags- oder Leistungsverhältnis zur AHV hatten (Art. 50c).

Im gleichen Artikel, Abs 3, steht "Die Zusammensetzung der Versichertennummer darf keine Rückschlüsse auf die Person zulassen, der die Nummer zugewiesen wird."

Aktueller Stand

Es werden bereits heute in den verschiedensten Systemen die Daten von Personen mit ihren Identifikatoren verknüpft. Dabei sind nebst unproblematischen Infos wie Name oder E-Mail-Adresse häufig auch sensibelste Daten wie beispielsweise alle Gesundheitsdaten der Krankenkassen gespeichert.

Bekanntlich will der Bund auch für die E-ID den privaten Anbietern (wie zum Beispiel der privaten SuisseID) Zugang zur AHVN geben. Auf dieser E-ID, aber auch in vielen anderen Bereichen wie auch beim elektronischen Patientendossiers EPD, werden zunehmend auch biometrische Daten abgelegt: Von der Körpergrösse bis zu den Fingerabdrücken werden bald alle diese sehr persönlichen und besonders schützenswerten Daten gespeichert.

Wird die AHVN nun systematisch auch als Identifikator über weitere Ebenen der Anwendungen und Verwaltungstätigkeiten verwendet, hängt das ganze Leben respektive die komplette Identität des jeweiligen Inhabers immer wieder an derselben eindeutigen und einmaligen AHV-Nummer.

Risikoeinschätzung

Teilweise sind solche Datensätze in denselben Systemen gespeichert, teilweise in unterschiedlichen. Doch praktisch alle diese Systeme haben Gemeinsamkeiten:

- Sie laufen fast immer mit Standard-Software derselben paar Hersteller
- Sie laufen auf ähnlichen Computer-Infrastrukturen
- Praktisch alle Systeme sind immer online, also mit dem Internet verbunden

Somit haben alle Systeme auch ähnliche Risiken und es gibt unzählige Angriffsvektoren auf allen Ebenen dieser Systeme resp. Elemente. Bekanntlich

- sind heute weder Computer-Hardware noch Netzwerkgeräte sicher,
- noch sind alle Details von Betriebssystemen und Applikationen bekannt und kontrollierbar und
- private und staatliche Akteure sind zunehmend engagiert, alle möglichen Systeme und Datenbanken systematisch zu unterwandern.

Unseres Erachtens ist Ihre Einschätzung bezüglich Datenschutz und Risiken somit ungenügend.

Aufgrund obiger Punkte zieht die Piratenpartei Schweiz folgende Schlussfolgerung:

1. Je einheitlicher die Identifikationsmerkmale der verschiedenen Systeme sind, desto wahrscheinlicher ist das Risiko, dass diese Daten irgendwann von Unberechtigten zusammengeführt werden.
2. Werden die Daten irgend einmal zusammengeführt, können damit Personen und ganze Existenzen kontrolliert und zerstört werden.
3. Bezüglich Datenschutz hat die Schweiz bisher völlig unzureichende gesetzliche Grundlagen, so dass Verantwortlichkeits- und Haftungsfragen kaum entsprechende Konsequenzen haben.

Die Piratenpartei fordert deshalb explizit, die vorgeschlagene systematische Verwendung der AHV-Nummer durch Behörden zu verwerfen.

Im Weiteren fordern wir auch, die bereits bestehende Nutzung der AHVN stärker zu überprüfen und möglichst zu reduzieren. Alternativ würden wir die

- Neukonzeption der Datenbankarchitektur (1.3.2.1) oder die
- Sektoriellen Nummern (1.3.2.3) oder
- transaktionsbasierte Identifikatoren, wie bereits bei der E-ID Vernehmlassung gefordert

als bessere Lösungen im Sinne des Datenschutzes unterstützen.

Haftung und Verantwortlichkeit

Zusätzlich muss der Bund Möglichkeiten schaffen, um Personen mit gestohlenen Identitäten umfassend und unentgeltlich Hilfe zu leisten. Es ist auch Unterstützung zum Wechsel der Identifikatoren anzubieten, sofern eine Verwaltungstätigkeit Mitschuld am Identitätsdiebstahl hat. Die Verantwortlichkeits- und Haftungsfragen bei allen involvierten Akteuren sind ebenso vorgängig klar zu regeln.

Risikobeispiele

Beispiel von Klumpenrisiken:

- Die Post wird die SwissID mitbetreiben und -kontrollieren
- Die Post ist sehr engagiert im Bereich des elektronischen Patientendossiers EPD und verwaltet somit unzählige Patientendaten. Hier wird der Ersatz der Patientenidentifikationsnummer durch die AHVN bereits angestrebt.
- Die Post bemüht sich momentan stark darum, das E-Voting-Geschäft in der Schweiz als einziger verbleibender Anbieter umzusetzen. Eine Kopplung des Stimmrechts an die E-ID wird diskutiert.
- Dieselbe Post entwickelt andere strategische E-Government-Projekte der Schweiz (Strafregister-auszug, Beurkundung, Identitätsprüfung, etc.)
- Die Post betreibt nebenbei Lösungen für E-Commerce und kommerzialisiert zunehmend das Angebot in Filialen oder beim Onlinebanking mit individualisierten Promotionen.
- Die meisten dieser Systeme verwenden zur Identifikation die durch die Post abgeglichene Personen- und Adressdaten oder die AHVN, welche problemlos verknüpft werden könnten.

Die Post mit allen ihren Projekten ist somit ein Daten-Klumpenrisiko, da bei all diesen Geschäften immer wieder auf ähnliche Hardwarelösungen, Systemarchitekturen, Datenbanken, Softwarelösungen oder sogar Personen zurückgegriffen wird.

Somit kann die Post selbst oder ein externer staatlicher oder privater Akteur gezielt einzelne Schwachstellen ausnützen, um das allumfassendste Personen-Identitäts-Register der Schweiz aufzubauen und zu missbrauchen.

Ein solcher Schaden wäre unentschuldbar und irreversibel.

Die IT-Sicherheit ist niemals 100% gewährt: Kein Computer ist sicher, das Internet ist unsicher und die Rest-Risiken sind unkalkulierbar. Und die Schweiz ist dagegen leider auch nicht immun. Dass solche Vorfälle möglich sind wird in trauriger Regelmässikeit belegt. Bei der Post stürzen Drohnen vom Himmel, unsichere Verleihvelo-Schlösser werden auf den Markt gebracht, und Identitätsdiebstähle

- in den USA (https://www.newsweek.com/us-government-website-leaked-social-security-numbers-1103523)
- und (https://www.heise.de/newsticker/meldung/NASA-Moeglicherweise-jede-Menge-Mitarbeiterdaten-gehackt-4257068.html)
- oder in Indien (https://futurezone.at/digital-life/sozialversicherungsnummern-von-hunderttausenden-im-internet/400395923)

belegen, dass die extensive Verwendung von Sozialversicherungsnummern zu unkontrollierbaren Problemen mit Datenschutz, Identitätsdiebstahl und in der Folge zu Betrügereien führt.

Gerne verweisen wir diesbezüglich auch auf die Argumentation in der Vernehmlassungsantwort vom Verein grundrechte.ch welche wir vollumfänglich unterstützen sowie das Gutachten «Risikoanalyse zur unterschiedlichen Verwendung der schweizerischen AHV-Nummer» von Prof. Dr. David Basin, ETH Zürich.

———

Piratenpartei Schweiz, Arbeitsgruppe AHV-Nummer, 22. Februar 2019