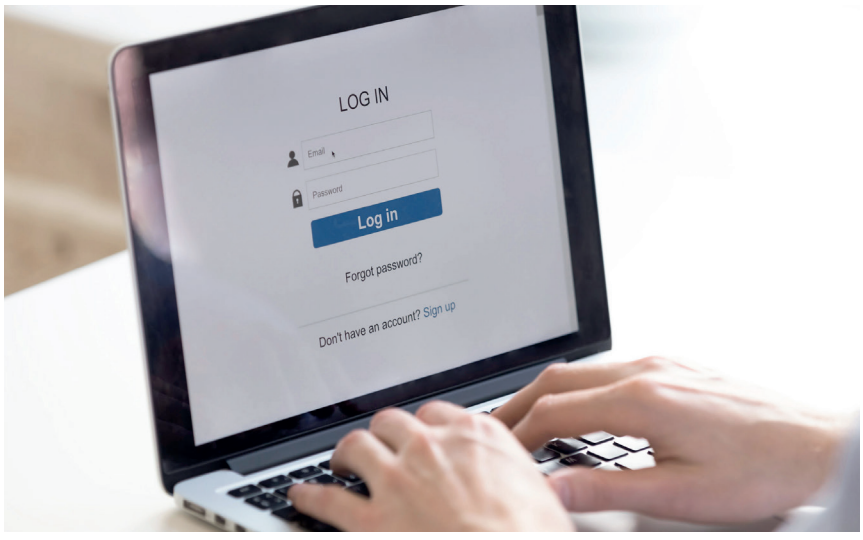
Standards helfen, Identitäten und personenbezogene Daten sicher zu verwalten

Wie sieht ein erfolgreiches Identity Access Management in der föderalen Schweiz aus? Wie gelangt die öffentliche Hand zu einheitlichen und durchgängigen Lösungen? Entscheidend sei der politische Wille, solche zu entwickeln und umzusetzen, betonten Fachleute an einem Anlass des Vereins eCH.

Wenn man online einkauft, Rechnungen zahlt oder eine Versicherung abschliesst, muss man sich ausweisen. Für ein Kundenkonto muss man personenbezogene Angaben machen. Je nach Anbieter muss man neben dem Namen eine E-Mail-Adresse, das Geburtsdatum oder die AHV-Nummer angeben. Um einzelne digitale Services zu nutzen, loggt man sich mit einem Passwort ein. Durch Identity und Access Management (IAM) wird sichergestellt, dass tatsächlich nur die eindeutig identifizierte und autorisierte Person zugelassen wird. Ist eine Anwendung mit sensiblen Daten verbunden, müssen die Benutzerverwaltung, das Anmeldeverfahren und die Vergabe von Zugriffsrechten besonders sicher ausgestaltet sein.



Dies ist unter anderem bei Patienteninformationen, E-Steuerrechnungen sowie Wahlen und Abstimmungen der Fall. Der Bundesrat und das Parlament möchten für entsprechende Online-Dienste eine staatlich anerkannte und geprüfte E-Identifikation schaffen. Das Stimmvolk wird voraussichtlich im März 2021 über das Bundesgesetz über elektronische Identifizierungsdienste (BGEID) entscheiden, welches die Grundlagen festhält. „Wir sind privilegiert“, sagte Peter Fischer, Präsident des Vereins eCH kürzlich in Bern. „Mir ist kein anderes Land bekannt, in dem man über einzelne Bausteine der Digitalisierung abstimmen kann.“

Dennoch gab die Umsetzung eines föderalen IAM an der traditionellen Abendveranstaltung viel zu reden. „Ein IT-Projekt ist unter anderem dann erfolgreich, wenn es die Erwartungen erfüllt“, sagte Daniel Muster, stellvertretender Leiter der eCH-Fachgruppe IAM. Problematisch sei es, wenn diese widersprüchlich oder falsch seien. Es werde etwa erwartet, dass ein Prozess anonym und gleichzeitig vertraulich ablaufe. Digitale Dienstleistungen sollten benutzerfreundlich, sicher und dennoch kostengünstig sein. „Das geht nicht zusammen.“

Biometrische Daten können nicht ersetzt werden

Der Referent appellierte daran, Authentisierung und Identifizierung strikte auseinanderzuhalten. Grund dafür sind Sicherheitsüberlegungen. Eine PIN, eine SmartCard oder eine SecureID, die zur Anmeldung eingesetzt wird, ist übertragbar. Wird sie missbraucht, kann sie widerrufen werden. Bei Merkmalen zur Identifizierung besteht diese Möglichkeit nicht. Gelangen biometrische Daten in falsche Hände, können sie nicht für ungültig erklärt und ersetzt werden. Auf eine Frage aus dem Publikum stellte Daniel Muster daher klar: „Man sollte biometrische Daten nicht auf unsicheren Geräten speichern.“ Er erwähnte Indien, wo der Staat die Kontrolle über die biometrischen Daten seiner Einwohner verloren hat. Die Personendaten von 1.2 Milliarden Menschen sind von Hackern kopiert worden. In Schweizer Gesetzen – darunter dem BGEID – werde Authentisieren häufig mit Identifizieren gleichgestellt, kritisierte Daniel Muster.

Dabei werde bei ersterem lediglich die Verantwortlichkeit zugeordnet. Es sei wie auf der Strasse: Aufgrund eines Nummernschilds lasse sich auf den Halter eines Fahrzeugs schliessen, nicht aber auf den Lenker.

„Es braucht Spielregeln und Leitplanken“

Bund, Kantone und Gemeinden verwenden heute zahlreiche IT-Systeme und erfassen unterschiedliche Personen- und Login-Daten. „Es gibt extrem viele Lösungen“, sagte Christian Grundlehner, Application Manager bei Abraxas. Diese seien oft nicht miteinander kompatibel. Beim Verwalten und Austauschen der Benutzerdaten ergäben sich Sicherheitsprobleme. Auch die Vertraulichkeit, die Berechtigung und die Kosten stellten in einem föderalen System eine besondere Herausforderung dar. „Akzeptanz ist der Schlüssel“, sagte Grundlehner. eGovernment-Services müssten sicher, günstig und intuitiv sein. Dafür brauche es Spielregeln und Leitplanken, wie sie der Verein eCH vorgebe.

Auch Stephen Tallowitz, Projektleiter Informatik Aargau, hob die Bedeutung von Standards hervor. „In einem föderalen System sind sie entscheidend“, sagte er. Es lohne sich, sie einzufordern. Im IAM seien SAML 2 (Security Assertion Markup Language) und Open ID connect weit verbreitet; sie würden von zahlreichen Programmiersprachen und Frameworks unterstützt. „Sie sind eine gute Basis, reichen aber nicht aus“, so der Referent. „Die Standardisierung muss weitergehen.“ Der Kanton Aargau hat 2014 damit begonnen, ein zentrales Login für verschiedene Applikationen anzuwenden. Seit diesem Jahr kann es auch mit externen Identitäten wie der SWISS-ID genutzt werden – vorerst im Pilotbetrieb und auf freiwilliger Basis. „Um nicht Dutzende externe Identity Provider einzubinden, braucht es eine klare Strategie“, betonte Stephen Tallowitz

Intensiv über strategische Entscheide diskutiert

In der abschliessenden Diskussion war man sich einig: Die öffentliche Verwaltung komme digital nur voran, wenn das politische Bekenntnis dazu da sei. „Technisch ist vieles möglich, aber es braucht ein paar Grundsatzentscheide der Politik“, sagte ein Anwesender. „Wieso machen wir es nicht wie Dänemark oder Estland?“, wollte ein anderer wissen. Die beiden Länder hätten den Durchbruch einigermassen geschafft, bestätigte Peter Fischer, Präsident des Vereins eCH und Leiter des Informatiksteuerungsorgans des Bundes (ISB). In Estland habe der Staat die gesamte Verwaltung aller Stufen und den Finanzsektor früh dazu verpflichtet, das gleiche IAM-System zu nutzen. „Es funktioniert, weil es flächendeckend umgesetzt wird.“

IT Architekt Michael Gerber erklärte, wie der SwissPass der SBB zu einem Erfolg wurde. „Im Verbund war der Wille da, vorwärts zu machen.“ Da die Lösung nutzerfreundlich und kostenlos sei, finde sie grossen Anklang. Einzelne strategische Entscheide hätten allerdings Zeit gebraucht. So hätten die Verantwortlichen beispielsweise ein Jahr lang darüber diskutiert, ob andere Online-Dienste des öffentlichen Verkehrs einbezogen sollen und nur noch das SwissPass Login verwendet werden soll. „Technisch wäre das schon früher machbar gewesen.“

„Dem Wettbewerb stellen“

Viele Unternehmen bemühten sich darum, für uns unsere einzige ID bereitzustellen, sagte Andreas Spichiger, Leiter Architektur beim ISB und Leiter der eCH-Fachgruppe SEAC (Swiss E-Government Architecture Community). Der User überlege sich, wovon er den grössten Nutzen habe. „Diesem Wettbewerb muss sich die öffentliche Verwaltung stellen.“ Spichiger sprach sich für eine föderierte ID-Lösung aus. Das Management der Identitäten und der personenbezogenen Daten muss seiner Meinung nach bei den Behörden bleiben. Eine Google- oder Facebook-ID sollte höchstens der Authentisierung dienen. „Wir schieben uns gegenseitig den Ball zu“, sagte Thomas Alabor, Vorstandmitglied von eCH, nach dem engagierten Austausch. Damit sich verschiedene Anwendungen mit korrekten Merkmalen abgleichen könnten, brauche es eine persönliche Erstidentifizierung durch die Bürgerinnen und Bürger. „Das bedeutet Aufwand“, räumte der Diskussionsleiter ein. „Aber daran führt wohl kein Weg vorbei.“

Eveline Rutz, Freie Journalistin. *Dieser Text ist im Auftrag von eCH entstanden.*

Der Verein eCH führt einmal jährlich eine offene Abendveranstaltung zu E-Government und Standardisierung durch. Die Abendveranstaltung 2020 stand unter dem Titel „Identity Access Management in einem föderalen System: Was ist der Schlüssel zum Erfolg?“

---

eCH Verein für E-Government Standards
Geschäftsstelle: Mainaustrasse 30 | Postfach | 8034 Zürich
Tel.: +41 44 388 74 64 | info@ech.ch | www.ech.ch