

Ein Pionier im Fokus – serviceorientierte Sicherheitsinfrastruktur im Kanton Aargau

Marco Bürli, Michael Liebi

Im Fokus aller E-Government-Vorhaben steht stets der Kundennutzen. Ein reibungslos funktionierendes Identity- und Access-Management (IAM) ist dabei ein zentraler Erfolgsfaktor, um die Zugriffe der Benutzerinnen und Benutzer mit unterschiedlichen Rollen auf die verschiedensten Anwendungen sauber umsetzen zu können. Das Beispiel des Kantons Aargau zeigt, wie eine zentralisierte und spezialisierte Sicherheitskomponente die Effizienz und die Flexibilität der E-Government-Vorhaben erhöht und welche Perspektiven sich damit eröffnen.



Marco Bürli
Leiter E-Gov-Projekte
Kanton Aargau
marco.buerli@ag.ch



Michael Liebi
CEO
United Security Providers AG
michael.liebi@united-security-providers.ch

Authentisierung – Schutz der Applikationen

Verwaltungen sind im E-Government zu einem grossen Teil mit denselben IAM-Anforderungen konfrontiert, wie sie bereits aus der Wirtschaft bekannt sind. Die E-Government-Anwendungen müssen adäquat vor unautorisierten Zugriffen und Angriffsversuchen geschützt bleiben. Der Betrieb in einer speziell gesicherten Netzwerkzone ist ein erster Schritt dazu. Dadurch erfolgt der Zugriff auf die Applikationen via Web nicht mehr direkt, sondern immer über eine separate Sicherheitsschicht. Diese Sicherheitsschicht prüft sämtliche Anfragen in ihrem jeweiligen Anwendungskontext, erkennt Attacken über mehrere Stufen und wehrt sie ab. Zudem authentifiziert sie die Benutzerinnen und Benutzer und regelt deren Zugriffe auf die Anwendungen von einer zentralen Stelle aus. Die Authentisierung unterstützt so auch die hohe Verfügbarkeit der E-Government-Dienste.

Autorisierung – Management von Zugriffsberechtigungen

Benutzerinnen und Benutzer mit unterschiedlichsten Berechtigungen greifen auf verschieden klassifizierte Anwendungen und Daten zu. Deshalb sind nach Schutzbedarf und Klassierung abgestufte Trust-Levels meist ein sinnvolles Konzept. Der von den einzelnen Anwendungen separierte Authentisierungsservice in der Sicherheitsschicht ermöglicht es – abgestimmt auf die verschiedenen benötigten Trust-Levels –, unterschiedliche Authentisierungsstärken pro Anwendung flexibel auszugestalten. Eine grosse Vereinfachung wird durch rollenbasierte Zugriffssteuerungen erreicht. Die Zuweisung von Rollen an Benutzende (User Provisioning) inklusive Nachvollziehbarkeit der Berechtigungsvergaben ist ein Kernprozess von Identity- und Access-Management.

Verwaltungsspezifische Herausforderungen

Die oben beschriebene Komplexität ist aus IAM-Projekten in grösseren Organisationen

der Privatwirtschaft bekannt, wo der Trend zum Einsatz von Intranets, Extranets und Kundenportalen schon länger besteht. Verwaltungen jedoch stehen oftmals vor zusätzlichen Herausforderungen: Der Zeitdruck für die Bereitstellung neuer und medienbruchfreier Dienstleistungen nimmt zu. Die Realisierungszeiten verkürzen sich, und die Ansprüche von Bürgerinnen und Bürgern sowie von Institutionen und Unternehmen steigen rasch. Viele Kantone haben mittlerweile eine eigene E-Government-Agenda und arbeiten gemeinsam mit dem Bund an den Umsetzungen von priorisierten Vorhaben.

Eine verwaltungsspezifische Herausforderung liegt darin, dass in E-Government-Projekten typischerweise verschiedenste Departemente involviert sind. Dabei kommen oftmals Applikationen zum Einsatz, die historisch bedingt auf die Bedürfnisse der Departemente zugeschnitten wurden. Im Gegensatz zur Wirtschaft werden insgesamt weniger oft Standardapplikationen eingesetzt. Auch aus föderalen Gründen und weil viele IT-Abteilungen dezentral geführt werden, herrscht tendenziell eine sehr hohe Applikationsvielfalt. Die individuelle Anpassung einzelner proprietärer Applikationen an die Sicherheitsanforderungen ist aufwendig und im Falle von Legacy-Systemen oft gar nicht möglich oder zumindest nicht wirtschaftlich. In jedem Fall beeinträchtigen Anpassungen an einzelnen Applikationen die Effizienz der E-Government-Vorhaben. Die Sicherheitsschicht muss entsprechend leistungsfähig sein, um diesem Umstand zu begegnen.

Zentralisierte Sicherheitsinfrastruktur

Die Auslagerung der Sicherheitsaspekte in eine spezialisierte Komponente ist für Verwaltungen eine attraktive Möglichkeit, die zuvor erwähnten vielfältigen Herausforderungen optimal zu lösen. Die geforderten Funktionalitäten zur Gewährleistung der Sicherheit stehen so an einer zentralen, spezialisierten Stelle in Form eines abonnierbaren Services zur Verfügung und kön-

nen mehrfach wiederverwendet werden. Der Grundgedanke der Serviceorientierung ist deshalb für Verwaltungen eine Erfolg versprechende Strategie.

Erfolg dank Serviceorientierung beim Kanton Aargau

Der Kanton Aargau gehört in der Schweiz mit seinen zahlreichen bereits umgesetzten Vorhaben zu den aktiven Kantonen in Sachen E-Government. Auch beim Kanton Aargau sind zahlreiche Departemente mit unterschiedlichsten Anforderungen in E-Government-Projekte involviert. Eine zentrale Anforderung an alle Komponenten der aargauischen E-Government-Infrastruktur war deshalb, dass sie für sämtliche Departemente nutzbar sind. Dieser Umstand begründete den Entscheid, die E-Government-Infrastruktur in einer serviceorientierten Architektur aufzubauen. Im Fokus standen auch die Überlegungen zu den Sicherheitsaspekten, die als wichtiger Bestandteil der Gesamtarchitektur bereits zu Beginn miteinbezogen wurden. Entsprechend entschied sich der Kanton Aargau für den Aufbau einer zentralen Access-Management-Lösung.

Access-Management

Die Access-Management-Lösung des Kantons Aargau umfasst sowohl den Zugriffsschutz als auch den Zugangsschutz in der kantonalen E-Government-Infrastruktur. Als zentraler Baustein der Architektur sollte sie deshalb eine breit gefächerte Funktionalität aufweisen:

- Die Access-Management-Lösung soll als zentrale Web Application Firewall den HTTP- und HTTPS-Datenverkehr bei den E-Government-Anwendungen überwachen, diese vor vielfältigen Attacken aus dem Internet schützen, insbesondere vor den OWASP-Top-10-Risiken, und so die Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Informationen gewährleisten.
- Als Authentifizierungsserver soll die Lösung verschiedenste Zugriffsmechanismen zentral abbilden und eine rollenbasierte Zugriffssteuerung unterstützen.
- Die Lösung muss eine serviceorientierte Architektur unterstützen. Dies bedeutet, dass die eingesetzten Produkte imstande sein sollen, sämtliche Funktionalitäten als zentrale Services zur Verfügung zu stellen.
- Die Sicherheitskomponente sollte einen späteren schrittweisen Weiterausbau der E-Government-Infrastruktur unterstützen.

Die Anmeldung der Kundinnen und Kunden am neu geschaffenen Onlineschalter unter www.ag.ch erfolgt vorgelagert auf der Access-Management-Lösung. Nimmt eine Kundin oder ein Kunde einen Service aus

dem Onlineschalter in Anspruch, werden interne Workflows angestoßen. Die zuständigen Mitarbeitenden können rollenbasiert die Workflows ihrer Fachabteilungen verarbeiten und steuern. Die Sicherheitskomponente kontrolliert, dass die Anwendungszugriffe nur mit korrekter Authentisierung und Autorisierung möglich sind.

«Der Vorteil unserer E-Government-Infrastruktur ist ihre Einfachheit. Diese wird durch eine klare Funktionstrennung erreicht – im Bereich Security ist dies die zentrale Authentisierung der Benutzerinnen und Benutzer, die von den dahinterliegenden Systemen entkoppelt wurde», erklärt Max Haefeli, CISO beim Kanton Aargau. Durch diese Sicherheitskomponenten kann ein Zugriff jederzeit nachvollzogen werden. Die Umsetzung der Vorgaben aus dem Standard ISO/IEC 27002, Kapitel 11.2 «Benutzerverwaltung», wird unterstützt. Nebst der entkoppelten Security-Komponente sind die zentral abgebildeten Prozesse ein weiteres wichtiges Konzept der Gesamtarchitektur. Die Workflows sind zentral abgebildet und bieten dem Kanton Aargau grösstmögliche Flexibilität, indem sie den einfachen Ausbau des Onlineschalters mit neuen elektronischen Verwaltungsprozessen erlauben. Im Onlineschalter unter www.ag.ch können heute bereits über 70 unterschiedliche Verwaltungsgeschäfte eingesehen und viele davon elektronisch abgewickelt werden. Mit 23 weiteren Vorhaben wird das E-Government-Angebot zurzeit intensiv ausgebaut.

Identity-Management – Prozesse weiter vereinfachen

Mit der intensiven Nutzung der E-Government-Services durch die Kundinnen und Kunden und mit dem dadurch erreichten Erfolg wachsen das Bedürfnis und die Notwendigkeit, die Effizienz «im Backoffice» zu steigern und die IT-Unterstützung rund um eine moderne Identitäts-, Rollen- und Rechteverwaltung zu erweitern. So will der Kanton Aargau seine Sicherheitsarchitektur durch eine neue Identity-Management-Lösung ergänzen, die sich in die bestehende, wachsende und stark am Kundennutzen ausgerichtete Architektur einfügt. Diese wird die Verwaltung von Identitäten und Rollen wie Bürgerinnen und Bürger, Kantonsmitarbeitende, Gemeindemitarbeitende vereinfachen und die aktuellen Standards unterstützen (u. a. eCH-0107 Version 2.0).

Der Kanton Aargau ist bereit für die Zukunft

Der langfristige Nutzen einer integrierten Sicherheitsinfrastruktur zeigt sich bei der Betrachtung der laufenden Projekte. Die durch die Digitalisierung der Verwaltungsprozesse erreichte Industrialisierung soll sich zukünftig auch in der zwischenbehörd-

lichen Zusammenarbeit zeigen. Dazu ist eine verbesserte Interoperabilität zwischen verschiedenen Serviceanbietern gefordert, insbesondere bei der Benutzerauthentisierung. Deshalb wird in einem nächsten Ausbauschritt das Thema Federated Identity bearbeitet. Dahinter steckt die Grundidee, dass die eigentlichen Benutzerinformationen dort verbleiben, wo die Datenhoheit besteht. Erreicht wird dies durch den Einsatz des SAML-2.0-Standards, der als interoperables XML-Protokoll den Austausch von Authentisierungs- und Autorisierungsinformationen von Identitäten zwischen verschiedenen Control-Domains ermöglicht. Auf diese Weise können Verwaltungsstellen und Behörden sowie autorisierte Wirtschaftsunternehmen ihre Zusammenarbeit auf der Basis von etablierten technischen und organisatorischen Standards vereinfachen und effizienter gestalten. So ist es beispielsweise in Zukunft möglich, dass sich Mitarbeitende des Strassenverkehrsamts des Kantons Luzern beim Strassenverkehrsamt des Kantons Aargau Benutzeridentitäten gespeichert sind.

Kanton Aargau als Service-provider

Dank der konsequenten Verfolgung des Paradigmas der Serviceorientierung verfügt der Kanton Aargau heute über eine E-Government-Infrastruktur, die aufgrund eines reibungslosen Zusammenspiels der einzelnen, spezialisierten Komponenten eine höchstmögliche Skalierbarkeit und Flexibilität aufweist. Auf dieser Grundlage arbeitet der Kanton Aargau an Shared Services für seine Gemeinden und andere Verwaltungen. Durch die Nutzung der serviceorientierten, modular aufgebauten Infrastruktur des Kantons Aargau können in Zukunft auch andere Anspruchsgruppen ihre E-Government-Vorhaben effizient umsetzen.

Fazit

Mit der Weiterverfolgung der oben aufgezeigten Vorhaben im Bereich Identity-Management, Federated Identity und Shared Services wird der Kanton Aargau seine aktive Rolle auch in den nächsten Jahren beibehalten und seinem Anspruch, ein fortschrittlicher Wohn- und Wirtschaftskanton zu sein, weiterhin gerecht werden.